ENHANCING PHYSICAL LAYER SECURITY IN COGNITIVE RADIO NETWORKS

Al-Talabani, Ali Mohammed Noori Hasan

Awarding institution:
King's College London

ENHANCING PHYSICAL LAYER SECURITY IN COGNITIVE RADIO NETWORKS

ALI AL-TALABANI

KING'S COLLEGE LONDON

2016

ENHANCING PHYSICAL LAYER SECURITY IN COGNITIVE RADIO NETWORKS

ALI AL-TALABANI

(*M.Sc. in Electronics and Communication Engineering*)

A THESIS SUBMITTED

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRONIC ENGINEERING

KING'S COLLEGE LONDON

2016

Dedication:

To My Mother

Acknowledgements

First, I would like to thank Prof. Arumugam Nallanathan for his valuable guidance and support throughout the my PhD studies. His advice, patience, kind supervision, and encouragement over my study period have been vital for the completion of this thesis.

I would also like to thank my secondary supervisor, Dr. Vasilis Friderikos, for his kind support and friendship, as well as Dr. Yansha Deng and Dr. Huan Nyguen for their support and advice. My warmest thanks go to my colleagues and the staff at the Centre for Telecommunications Research at King's College London for their friendship and help throughout my PhD studies.

Finally, I would like to deeply thank my family, and especially my wife, for their love, support, and encouragement.

Contents

Abstract

A cognitive radio is an intelligent wireless communication system that improves spectrum utilisation by allowing secondary users to use the idle radio spectrum from primary licensed networks or to share the spectrum with primary users. Due to several significant challenges for cryptographic approaches of upper layers in protocol stacks — for example, private key management complexity and key transmission security issues — physical layer (PHY) security has drawn significant attention as an alternative for cryptographic approaches at the upper layers of the protocol stack. Security threats may arise from passive eavesdropping node(s), which try to intercept communications between authenticated nodes. Most recent studies consider information theoretic secrecy to be a promising approach. The idea of information theoretic secrecy lies in exploiting the randomness of communication channels to ensure the secrecy of the transmitted messages. Due to the constraints imposed on cognitive radio networks by secondary networks, allocating their resources in an optimal way is a key to maximising their achievable secrecy rates. Therefore, in this thesis, optimal resource allocation and secrecy rate maximisation of cognitive radio networks (CRNs) are proposed.

Cooperative jamming is proposed to enhance the primary secrecy rate, and a new chaos-based cost function is introduced in order to design a power control algorithm and analyse the dynamic spectrum-sharing issue in the uplink of cellular CRNs. For secondary users as the game players in underlay scenarios, utility/cost functions are defined, taking into account the interference from and interference tolerance of the primary users. The existence of the Nash equilibrium is proved in

this power control game, which leads to significantly lower power consumption and a relatively fast convergence rate when compared to existing game algorithms. The simulation results indicate that the primary secrecy rate is significantly improved by cooperative jamming, and the proposed power control algorithm achieves low power consumption.

In addition, an integrated scheme with chaotic scrambling (CS), chaotic artificial noise, and a chaotic shift keying (CSK) scheme are proposed in an orthogonal frequency division multiplexing (OFDM)-based CR system to enhance its physical layer security. By employing the chaos-based third-order Chebyshev map to achieve the optimum bit error rate (BER) performance of CSK modulation, the proposed three-layer integrated scheme outperforms the traditional OFDM system in an overlay scenario with a Rayleigh fading channel. Importantly, under three layers of encryption that are based on chaotic scrambling, chaotic artificial noise, and CSK modulation, a large key size can be generated to resist brute-force attacks and eavesdropping, leading to a significantly improved security rate.

Furthermore, a game theory-based cooperation scheme is investigated to enhance physical layer (PHY) security in both the primary and secondary transmissions of a cognitive radio network (CRN). In CRNs, the primary network may decide to lease its own spectrum for a fraction of time to the secondary nodes in exchange for appropriate remuneration. The secondary transmitter (ST) is considered to be a trusted relay for primary transmission in the presence of the ED. The ST forwards a message from the primary transmitter (PT) in a decode-and-forward (DF) fashion and, at the same time, allows part of its available power to be used to transmit an artificial noise (i.e., jamming signal) to enhance secrecy rates. In order to allocate power between the message and jamming signals, the optimisation problem is formulated and solved for maximising the primary secrecy rate (PSR) and secondary secrecy rate (SSR) with malicious attempts from a single eavesdropper or multiple eavesdroppers. Cooperation between the primary and secondary transmitters is also analysed from a game-theoretic perspective, and

their interaction modelled as a Stackelberg game. This study proves theoretically and computes the Stackelberg equilibrium. Numerical examples are provided to illustrate the impact of the Stackelberg game-based optimisation on the achievable PSR and SSR. The numerical results indicate that spectrum leasing, based on trading secondary access for cooperation by means of relay and a jammer, is a promising framework for enhancing primary and secondary secrecy rates in cognitive radio networks when the ED can intercept both the primary and secondary transmission.

Finally, this thesis focuses on physical-layer security in cognitive radio networks where multiple secondary nodes assist multiple primary nodes in combating unwanted eavesdropping from malicious eavesdroppers. Two scenarios are considered: a single eavesdropper (scenario I) and multiple eavesdroppers (scenario II). The secondary users act as a relay and jammer in scenario I, whereas they act only as a jammer in scenario II. Furthermore, the multiple eavesdroppers are distributed according to a homogenous Poison Point Process (PPP) in scenario II. Closed forms are derived for the outage probability and mean secrecy rate for both the primary and secondary transmissions. Furthermore, the scalability and convergence of the matching theory are proved. Both the analytical and numerical results show that the proposed matching model is a promising approach for exploiting the utility functions of both primary and secondary users.

List of Figures

List of Notations

a, A	letters denote scalars
$\mathbf{a}, \mathbf{A}$	boldface letters denote vectors
$(\cdot)^\dagger$	conjugate transpose of a matrix
$\mathbb{E}\{\cdot\}$	statistical expectation operator
$\mathbf{x} \preceq \mathbf{y}$	componentwise inequality between vectors $\mathbf{x}$ and $\mathbf{y}$
$[x]^+$	$\max(0, x)$
$\mathrm{Re}\{\cdot\}$	real part of the argument
P	power
$\mathbb{P}$	probability
$\mathcal{CN}(0, \sigma^2)$	circularly symmetric complex Gaussian random variable with mean zero and variance σ^2
$\Gamma(\cdot)$	gamma function
$\arg\max[f(x)]$	value of x that maximizes the function $f(x)$
$\log(\cdot)$	natural logarithm
$\log_x(y)$	logarithm, base x, of y
$\exp(x)$	e^x

List of Abbreviations

PHY	Physical Layer
CRNs	Cognitive Radio Networks
SU	Secondary User
PU	Primary User
CS	Chaotic Scrambling
CSK	Chaotic Shift Keying
DCSK	Differential Chaotic Shift Keying
GA	Gaussian Approximation
OFDM	Orthogonal Frequency Division Multiplexing
C-OFDM	Chaotic Orthogonal Frequency Division Multiplexing
CR	Cognitive Radio
BER	Bit Error Rate
ST	Secondary Transmitter
SR	Secondary Receiver
PT	Primary Transmitter
PR	Primary Receiver
ED	Eavesdropper
DF	Direct and Forward
PSR	Primary Secrecy Rate
SSR	Secondary Secrecy Rate
PPP	Poison Point Process
CSI	Channel State Information
SINR	Signal to Interference and Noise Ratio

QOS	Quality of Service
PSMA	Primary Secondary Matching Algorithm

Chapter 1

Physical layer security in cognitive radio networks

1.1 Introduction

The radio frequency spectrum is becoming scarce due to the low utilisation of spectrum resources under conventional fixed-spectrum allocation schemes. According to the Federal Communications Commission (FCC), temporal and geographical variations in the utilisation of the assigned spectrum range from 15% to 85% [1]. The limited available spectrum and the inefficiency of spectrum usage necessitate a new communication paradigm, cognitive radio (CR), to exploit the flexible spectrum [2]. As an intelligent wireless communication system, a secondary transmitter can sense the radio frequency environment, adjust its transmit parameters, such as carrier frequency, bandwidth, and transmission power, to optimise spectrum usage, and adapt its transmission and reception accordingly. Developing advanced transceivers for the physical layer is a key objective in the successful deployment of CR systems. Spectrum pooling is an opportunistic spectrum access approach that enables public access to licensed frequency bands [3, 4]. Spectrum pooling merges spectral resources from different spectrum owners (for example, military radios) into a common pool, from which secondary users

may temporarily access idle spectral resources of licensed users. In this case, the transmission of the licensed users is not influenced by the secondary transmission, and the licensed system remains the same. Broadcast, a fundamental characteristic of the wireless network, causes several challenges for ensuring secure communications in the presence of eavesdroppers. The broadcast nature of wireless communications makes it difficult to shield the transmitted signals from illegal recipients. As a consequence, attackers are well-known and modeled either as (1) an unauthorised receiver (eavesdropper) that attempts to extract information from the receiving signal of a legal transmission without being detected, or (2) a malicious transmitter (jammer) that sends a jamming signal to degrade the signal-to-noise ratio at the legal receiver [10, 35]. Recently, physical layer (PHY) security has attracted significant attention as an alternative for cryptographic algorithms at the upper layers of the protocol stack in secure communication systems [36–38]. Security threats may be induced by passive eavesdropping node(s) which try to intercept communication between authenticated nodes. Traditionally, there have been several significant challenges for cryptographic approaches of upper layers in protocol stacks, such as private key management complexity, key distribution obstacles, and key transmission security issues. Recent years have seen the development by Wyner in [39] of a promising approach for achieving secure communications: information theoretic secrecy. The power of information theoretic secrecy lies in exploiting the randomness of communication channels to ensure secrecy for transmitted messages.

In this chapter, an overview is provided of existing algorithms and methods for improving PHY security in CRNs. Recent developments and challenges in PHY security are then discussed, and finally the contributions and organisation of this thesis are presented.

1.2 Cognitive radio technology

Among many potential technologies that enable the transmission of unlicensed users in spectrum-pooling radio systems, OFDM-based software defined radio

(SDR) provides significant flexibility for mixing the types of signal processing elements within the system, as OFDM provides the capability to multiplex multiple modulation types in each OFDM block. In each block, the format can be variable, potentially providing adaptive-channel, loading, and/or hierarchical service compensation [5]. The downlink channel assignment and power control problem for frequency-division, multiple-access (FDMA)-based cognitive radio networks was addressed in [6]. In the approach presented in [7], the base stations in each cell perform spectrum access according to the opportunistic principle in order to serve the secondary users (SUs) within their cells. Each SU can be either active or idle and a BS needs only one channel to support each active SU. To maximise the total number of active SUs that can be supported while guaranteeing the minimum signal-to-interference-plus-noise ratio (SINR) requirements of SUs, as well as protecting the primary users, suboptimal schemes are suggested for the formulated mixed integer program. In CR networks with the coexistence of multiple primary and secondary links via an orthogonal frequency-division multiple-access (OFDMA)-based air interface, the approach in [8] utilised the dual method that was proposed in [9] to provide centralised and distributed algorithms that improve the total achievable sum rate of secondary networks subject to interference constraints at the primary receivers. Formally, a CR is defined as a radio that can change its transmitter parameters depending on interactions with its environment. From this definition, two main features of cognitive radio (CR) emerge [2]. The first feature is cognitive capability; during real-time interaction with the radio environment, the unused portions of the spectrum at a specific time or location can be identified. CR enables occupation of the temporally idle spectrum according to the spectrum hole or white space. Consequently, the desired spectrum can be selected, shared with other users, and also exploited without interference with the licensed user. Secondly, CR exhibits re-configurability; a CR must be programmed to communicate on different frequencies and use multiple-access technologies, such as CDMA or OFDMA, as a physical layer in the transceiver design. According to this capability, the operating

parameters can be reconfigured to select the most appropriate spectrum. In order to provide the aforementioned capabilities, CR requires a novel radio frequency (RF) transceiver architecture. The main components of a CR transceiver are the radio front-end and the baseband processing unit, originally proposed for software-defined radio (SDR) (6.1). In the RF front-end the received signal is amplified, mixed, and converted from analog to digital (A/D). Modulation and demodulation of signals occurs in the baseband processing unit. Each component can be reconfigured via a control bus to adapt components' parameters according to the time-varying RF environment. The novel feature of the CR transceiver is the wideband RF front end, which enables simultaneous sensing over a wide spectrum. RF hardware technologies, such as a wideband antenna, power amplifier, and adaptive filter, can provide this functionality.

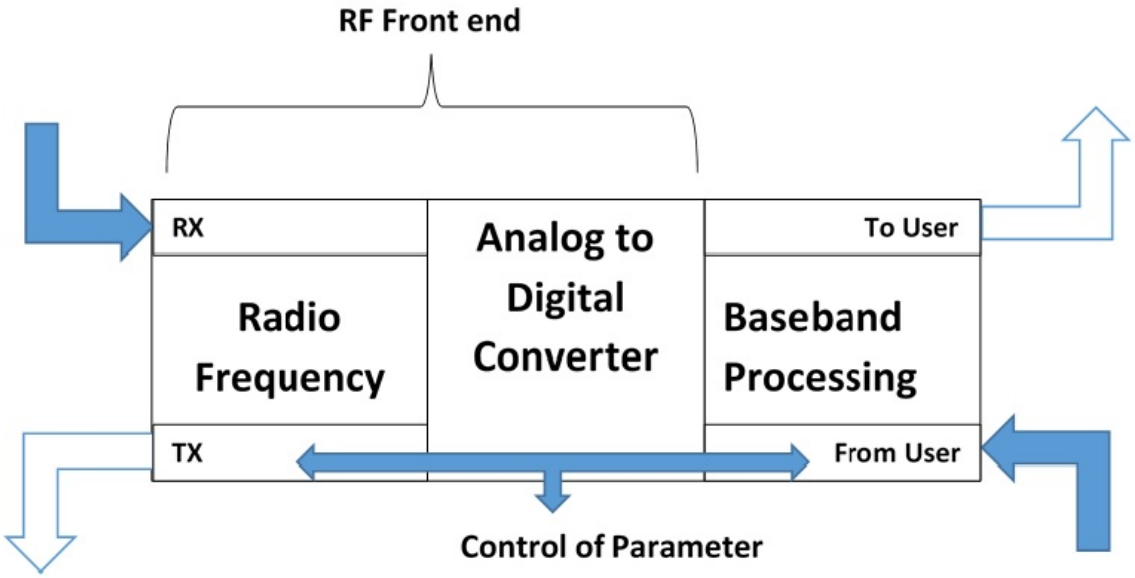

Figure 1.1: Architecture of a CR transceiver

.

1.3 PHY security in CRNs

In this section, previous contributions to PHY security in CRNs are discussed. In PHY security, the figure of merit is the secrecy rate, which is defined as the difference between the transmission rate of the source-destination link and that of the source-eavesdropper link. However, the secrecy rate will be equal to zero if the source-destination channel is worse than the source-eavesdropper channel. For a Gaussian channel, the achievable secrecy rate is equal to the difference between the mutual information accumulated at the destination and that accumulated at the eavesdropper (ED), which is not less than zero [40]. Recently, chaos-based cryptography has attracted significant attention for its implementation simplicity, complex behaviour, and extreme sensitivity to initial conditions. In [14], the scrambling matrix, based on a key derived from one-dimensional chaotic nonlinear dynamic system using logistic map, was considered.Two types of receivers have been proposed in chaos-based systems: coherent and non-coherent. In the chaotic shift keying (CSK) system with a coherent receiver, the chaotic signal is used to carry the data information signal, while chaotic synchronisation is required at the receiver in order to regenerate an exact replica of the chaotic sequence and demodulate the transmitted bits. In the differential chaotic shift keying (DCSK) system with a non-coherent receiver, chaotic synchronisation is not used on the receiver side [11]. In [11], it is illustrated that chaotic synchronisation poses a significant challenge for the demodulation process at the coherent receiver of a chaotic system.

In [21], the security performance of a DCSK system was improved by introducing a permutation transformation in time, which hides the similarity between the reference and data samples to make the bit rate undetectable from the frequency spectrum. Kaiser et al. proposed a multi-carrier-DCSK (MC-DCSK) system wherein N sub-carriers are modulated by a combined sequence between data and reference sequences. In this system, the chips are interleaved to increase the security of the transmission by randomly dispersing the chaotic chips of data symbols in the time and frequency domains. Thus, a diversity of orders corresponding to N

sub-carriers can be achieved, provided the channel offers this degree of diversity [22]. After eliminating the guard interval, OFDM demodulation, and chip de-mapping, the received signal is correlated to a delayed version (of the received signal) and summed over the symbol duration with any channel gains in the receiver being unknown. The received bits are estimated by computing the sign of the output of the correlator.

The proposed MC-DCSK system is robust against multipath fading [23], [24], and achieves enhanced secure transmission with suppressed narrowband interference. Many studies compute the bit error rate (BER) performance of MC-DCSK by considering the transmitted bit energy as constant [11] [26]. This approximation, widely known as the Gaussian approximation (GA), suffers from low precision when the spreading factor is low [27]. Kaddoum et al. in [29] extended the Gaussian approximation (GA) in [28] to compute a BER expression for the MC-DCSK in an $m-$distributed fading channel, taking into account the variation of the bit energy after spreading by the chaotic signal. Note that these studies only considered a single layer of security represented by DCSK to provide protection against brute-force attacks.

1.4 Scope of the thesis and related work

The main aim of this thesis is to improve the PHY security of cognitive radio systems by optimally allocating their available resources. Many recent studies have focused on the game theory-based cooperative jamming paradigm, as the open nature of the wireless medium makes it susceptible to malicious eavesdropping. In [41], the authors proposed cooperative jamming to counter this vulnerability to eavesdroppers. In cooperative jamming, interference is created by the network nodes to transmit noise or codewords that impair the ability of eavesdroppers to decode confidential information [42]. The authors in [43] considered the power allocation optimisation problem to maximise the secrecy rate in a two-hop wireless relay network. The authors in [44] maximised the secrecy rate of the primary

network while satisfying a required rate for the secondary network by using an optimal beamformer design at the secondary transmitter with multiple antennas. The study in [45] considered the secrecy rate maximisation problem based on game theory, whereby the jammer introduces pricing charges for its jamming service based on the amount of interference caused to the eavesdropper. This secrecy rate maximisation problem was formulated as a Stackelberg game with the jammer and the legitimate transmitter playing the roles of leader and follower in the game. In [46], the authors demonstrated that cooperative jamming leads to a substantial improvement in the secrecy rate. This study involved multiple potential jammers, with competition between them modelled for bandwidth access via distributed resource allocation mechanisms, such as auctioning and the power control game. With the goal of maximising the data transmission rate priced by the jammer's power, the transmit power of cooperative jammers is generally proportional to the amount of leased bandwidth. In [47], the authors considered a scenario wherein an external eavesdropper attempts to decode the primary user's message. The primary user allows the secondary user to share the primary user's spectrum to improve its own secrecy rate through cooperative jamming from the secondary user. A different setup is investigated in [48], in which the secondary user wants to keep its message confidential from the primary network, which means that the primary receiver is viewed as an eavesdropper from the perspective of the secondary network. In [49], the inner and outer bounds on the capacity equivocation region were derived. Recently, the interactions between agents (transmitters, receivers, helpers, and eavesdropper) in multiuser wireless networks were accurately captured by interdisciplinary analyses based on game theory. The main function of game theory is to model agents or players as rational entities whose sole focus to maximise their individual gains or payoff functions. In [55] and [56], a Stackelberg power-control game was proposed for the primary-secondary interactions, whereby the primary user permits secondary transmissions only to improve its own secrecy rate.

In [57], the authors proposed a zero-sum game between a multi-channel

transmitter and an adversary in the form of an eavesdropper, in which the payoff was the difference between Alice's and Eve's SINR. Using the secrecy rate as the payoff in a game theory is a relatively new concept. The authors in [58] studied a SISO wiretap network with an adversarial jammer helping the eavesdropper as a zero-sum game, and solved the Nash equilibrium along with the source and jammer cumulative distribution functions. In [59] and [60], the authors considered a MIMO wiretap channel with an active eavesdropper that could either listen or jam, and modelled its interactions with the legal transmitter as a zero-sum game with the MIMO secrecy rate as the payoff function. In [61], the SISO one-sided interference channel was presented, and the authors proposed a game-theoretic model wherein the payoff to each pair was their own secrecy rate, and derived the corresponding Nash equilibrium secrecy rate region. The authors in [62] modelled a zero-sum power allocation game between a multi-channel transmitter and a hostile jammer distinct from the eavesdropper, considering the secrecy rate as the payoff function. Cooperative game theory was studied in [63] to demonstrate the enhancement in secrecy capacity of an *ad hoc* network, when users create coalitions via collaborative beamforming, to nullify the signals overheard by eavesdroppers. For a hierarchical multi-hop system with different potential paths to the base station, a game-theoretic framework was proposed in which a number of nodes interact and select optimal and secure communication paths in the uplink of a wireless multi-hop network, in the presence of eavesdroppers; a distributed tree formation game was postulated to solve this game [64]. Han et al. [65] developed a Stackelberg game wherein a transmitter pays a number of external helpers to jam an eavesdropper, and indicated the corresponding equilibrium prices and convergence properties. The same authors proposed a distributive auction game in a similar scenario in [66], to model the transactions between transmitters and helping jammers. The authors in [67] applied pricing functions to improve the energy efficiency and sum secrecy capacity in an M-user non-cooperative power control game. Finally, in [68], game theory was proposed for the interaction between multiple eavesdroppers deciding whether or

not to collude in a MISO wiretap channel. The authors then indicated the necessary conditions for eavesdropper cooperation in an infinitely repeated game.

1.5 Contributions and organisation of thesis

The main contributions of this thesis include providing methods and algorithms that can enhance the achievable secrecy rate and secrecy outage in CRNs via cooperative jamming with chaotic optimisation and communication, a Stackelberg game, and matching theory. The remainder of this thesis is organised as follows. In Chapter 3, a resource allocation (i.e. power) scheme is proposed for spectrum leasing in underlay CRNs to maximise the primary secrecy rate with perfect knowledge of channel state information (CSI). A novel and efficient cost function based on a chaotic logistic map is proposed, which guarantees convergence of the '*power*' game to a unique Nash equilibrium. Power control is achieved with a significant reduction in power consumption for cognitive users (by at least half compared to other methods). It is also shown that the rate of convergence of the proposed chaotic algorithm is relatively fast compared to existing iterative methods. In Chapter 4, three-layer protection for CR networks is proposed. The first and second layers provide protection against brute-force attacks, while the third layer provides protection against eavesdroppers. The secrecy rate and the power allocation of the proposed C-OFDM CR networks are optimised under different scenarios for eavesdroppers. In Scenario 1 with a single eavesdropper, an efficient optimisation scheme is provided to maximise the secondary secrecy rate (SSR) under the flat fading channel model. Subsequently, the secondary power optimisation allocation problem is analysed and solved at the secondary transmitter (ST). In Scenario 2 with multiple eavesdroppers, an analysis is provided for the proposed CR systems under malicious attacks from multiple non-colluding eavesdroppers that are distributed according to a homogeneous Poisson point process (PPP) around secondary transceivers. This is to highlight the impact of multiple eavesdroppers on the primary secrecy rate (PSR) and SSR. It is shown that the secrecy outage probability and the mean

secrecy rate achieved for CR systems under the non-colluding eavesdroppers are significantly lower than under traditional transceivers without artificial noise. In Chapter 5, two schemes are proposed for applying the Stackelberg game to CRNs. In Scheme 1, novel system designs are proposed for power allocation and time allocation for primary and secondary transmissions that maximise the achievable PSR and SSR subject to a total transmit power constraint. In Scenario I, with a single eavesdropper, an efficient optimisation is provided that maximises both the PSR and SSR under the flat fading channel model. In particular, we analyse and solve the primary and secondary power allocation problems at the ST using time slot allocation of the spectrum lease. In Scenario I, the secrecy rates achieved with the proposed 3-phase system are higher than those in other studies ([37],[39]), which are based on an external jammer in the same geometric environment. In Scenario II, an analysis is presented of the proposed CRNs under malicious attempts by multiple eavesdroppers (colluding and non-colluding eavesdroppers) around the ST to highlight the impact of multiple eavesdroppers on the PSR and SSR. The power allocation problem and time allocation problem are analysed and solved. In Scenario II, it is shown that the secrecy rate achieved for CRNs under the colluding eavesdropper is significantly lower than that under non-colluding eavesdroppers. In Scheme 2, a resource allocation (i.e., power and time resources) scheme is proposed for spectrum leasing to maximise the primary secrecy rate (PSR), relay secrecy rate (RSR), and secondary secrecy rate (SSR) with perfect knowledge of channel state information (CSI). The unique value of the proposed Stackelberg game equilibrium is obtained. It is shown that the secrecy rate of the proposed system using a multi-level Stackelberg game is significantly higher than that using the single level Stackelberg game. Comparisons with previous work are provided to show the significant improvement to security in the proposed system. In Chapter 6, a utility-based matching framework is proposed to motivate multiple primary nodes and multiple secondary nodes to cooperate with each other such that the sum-secrecy rate over all source nodes is maximised. This study provides a novel

framework that can address the general matching scenario to enhance security for both primary and secondary transmissions. In Scenario 1 with a single eavesdropper, matching theory and auction theory are applied to the allocated secondary power to relay the primary message and create interference with the eavesdropper. Simulation results show that the proposed scheme provides a significant increase in the primary secrecy rate (PSR) at the expense of a slight reduction in the secondary secrecy rate (SSR) in comparison with the corresponding central algorithm. In Scenario 2 with multiple eavesdroppers, matching theory and auction theory are applied to the allocated secondary power to create interference with the eavesdroppers. Again, simulation results show that the proposed scheme provides a significant increase in the primary secrecy rate (PSR) at the expense of a slight reduction of the secondary secrecy rate (SSR) in comparison with the corresponding central algorithm. Finally, conclusions are drawn and future work is discussed in Chapter 6, and proofs of all lemmas are provided in the Appendices.

Chapter 2

Wireless Channel Models and Physical layer Security

2.1 Introduction

In recent years, security issues in cognitive radio networks (CRNs) have been a subject of growing interest [73],[74]. Security threats can, for example, arise in the presence of passive eavesdropping node(s) trying to intercept communication between authenticated nodes. A promising approach for achieving secure communications was developed by Wyner in [75]: information theoretic secrecy. The use of a friendly jammer to facilitate the degradation of the source-to-eavesdropper channel has been considered (see e.g., [76],[77]). This is achieved by a friendly jammer transmitting a jamming power signal, which has the effect of decreasing the signal-to-noise ratio at the eavesdropper. This approach is often referred to as cooperative jamming. In addition, multi-antenna systems have been an important research area because they offer high data transmission and increased reliability for wireless communications [78]. Previous studies have considered various scenarios for the sources, destinations, jammers, and eavesdroppers. For example, a scenario comprising a single source-destination pair, a single jammer, and a single eavesdropper was considered in [79], while a single source-destination pair,

multiple jammer, and single eavesdropper were considered in [80], ,[81]. The authors in [82] considered multiple source-destination pairs and a single eavesdropper, whereas a single source node, multiple destination nodes, and multiple eavesdroppers were considered in [83]. Another scenario was considered in [84] with a single source-destination pair, multiple jammers, and multiple eavesdroppers. In contrast to the single source-destination pair or single jammer scenarios in the literature, here the focus is on a more general scenario with multiple source-destination pairs, multiple jammers, and a single eavesdropper. In addition, most existing studies have assumed perfect channel knowledge from the source to the eavesdropper. This is valid only if the eavesdropper is part of the communication system. For example, in [85], a scenario was considered in which the receivers eavesdrop on the message intended for other receivers. However, in some cases, the eavesdropper may not be a user that is part of the system, and in such a case, obtaining the eavesdropper channel information would be difficult. In this regard, physical layer security with evesdroppers having partial or no channel state information (CSI) was considered in [86],[88] and [87]. In underlay CRNs, a primary service provider allows the reuse of its spectral resources by an unlicensed secondary system, provided that a specified, maximum tolerated interference level generated by the secondary transmitter is not violated. The open nature of the wireless medium makes the transmission susceptible to malicious eavesdropping, and as a result, many studies have focused on the cooperative jamming paradigm , which creates interference at eavesdroppers [95],[96]. The authors in [95] proposed secondary cooperation to maximise the secrecy rate of the primary network while satisfying a required secondary rate for the secondary network. This is achieved by an optimal design of a beamformer at the multiple-antenna secondary transmitter to generate interference to confuse an eavesdropper. In [96], the authors proposed cooperative jamming to counter this vulnerability caused by eavesdroppers. In cooperative jamming, network nodes create interference to transmit noise or codewords and thereby impede eavesdroppers' decoding of the confidential information. A primary

goal of CRNs is to provide transmission opportunities and a substantial quality of service (QoS) for SUs, and avoid interference harmful to PUs. Thus, power control is essential for CRNs, and has recently attracted considerable attention. In particular, power control in traditional wireless networks has been studied extensively. Earlier schemes, such as signal-to-noise plus interference ratio (SINR) balancing, which was initially proposed for satellite communications and then adapted to wireless communications, suffer from slow convergence [90]. The model in [91] proposed a cost for each mobile that consisted of a weighted sum of power and square of SIR error, and obtained the static Nash equilibrium for the resulting costs. Also, recent studies demonstrated the impact of channel knowledge on CR capacity, particularly the importance of channel state information (CSI) between the SU and the PU [93]. In [89], a new iterative algorithm was suggested using game theory. The authors considered not only the SINR requirement, as with other game theoretic algorithms, but also the influence of the power threshold. However, this algorithm suffers from an increase in power consumption. A new cost-based primary-secondary interaction model for cellular cognitive radio networks was proposed in [94]. The authors proposed new utility and cost functions for primary and secondary users, respectively, and additionally improved convergence and power consumption of secondary users, with users given the opportunity to switch between base stations. Characteristics of chaotic motion include ergodicity, randomization, and regularity, and hence all states of the mapping function can be traversed without repetition within a certain scope. Previous studies have applied chaotic variables to the optimisation search and have shown that it is useful for enhancing the convergence of random search-based optimisation [92]. The authors in [100] considered a four-node cognitive scenario wherein the secondary receiver (SR) is treated as a potential eavesdropper with respect to the primary transmission. The secondary transmitter can help the primary transmission, while guaranteeing that the primary message is not leaked to the secondary user(s). The authors investigated three different optimisation problems: maximisation of the primary

secrecy rate, maximisation of the secondary rate, and minimisation of the secondary transmit power. Furthermore, they analysed the cooperation between the primary transmitter (PT) and secondary transmitter (ST) from a game-theoretic perspective, in which interactions between the transmitters were modelled as a Stackelberg game. The primary and secondary users have their own interests and thus do not cooperate unconditionally. Non-cooperative game theory tools are a common approach to modeling their interaction in cognitive radio networks (CRNs) with secrecy constraints [101] or without secrecy constraints [102, 103]. An appropriate model for such scenarios is the Stackelberg game model [104] with the game leader selling some fraction of its spectrum and the follower awarded a share of the spectrum for its cooperation, as in [105]. Cooperative game theory was studied in [107] to demonstrate improvement in the secrecy capacity of an ad-hoc network when users form coalitions to nullify the signals overheard by eavesdroppers via collaborative beamforming. For a hierarchical multi-hop system with different potential paths to the base station, a distributed tree formation game was proposed in [108]. Han *et al.* [109] demonstrated a Stackelberg game in which a legal transmitter pays a number of external helpers to jam an eavesdropper, and computed the corresponding equilibrium prices and convergence properties. They also examined a similar scenario in [110], in which an auction game was used alternatively to model the transactions between transmitters and helping jammers. Anand and Chandramouli studied an M-user non-cooperative power control game with secrecy considerations in [111], and applied pricing functions to improve the energy efficiency and sum secrecy capacity of the network. Fakoorian *et al.* discussed in [112] and [113] how Kalai-Smorodinsky bargaining solutions and zero-sum games are adopted to allow the transmitters to find an operating point that balances network performance and fairness. In [114], game theory was used by multiple eavesdroppers to decide whether to collude or not in a MISO wiretap channel. The authors in [115] modelled the interaction between primary users and secondary users as a Stackelberg game in which transmission power levels are the key to maximi sing data rates. From these

studies, it can be shown that the ST can be utilised either as a relay to forward the primary information or as a jammer to send jamming signal. The goal is to enhance the primary secrecy rate and improve the secondary transmission rate.

2.2 Wireless Channel Model

Research studies into wireless communication systems demand background information in different aspects of wireless channel models. The mobile wireless channel can be defined as the variations of the channel strength over time and over frequency. The variations of the channel can be classified roughly into two classes. Firstly, large-scale fading, which yields due to the path loss of signal that considered as function of distance and shadowing by large objects such as hills, and it considers frequency independent. Secondly, small-scale fading which occurs due to the constructive and destructive interference of the multiple signal paths between the transmitter and receiver, and it considers frequency dependent.

2.2.1 The Wireless Channel as a Linear Time-Varying System

In a wireless communication, the channel refers to the dynamic and unpredictable characteristics of electromagnetic radiation which propagate from the transmitter (Tx) to the receiver (Rx). In 2.1. The three main physical phenomenon that occur when a signal is propagating in outdoor urban environments are reflection, diffraction and scattering. The received signal at Rx can be written as

$$\sum_i a_i(f,t)x(t-\tau_i(f,t)), \tag{2.1}$$

where $x(t)$ is the transmitted signal and $a_i(f,t)$ and $\tau_i(f,t)$ are the overall attenuation and propagation delay respectively at time t from the transmitter to the receiver on path i. In practice the attenuations and the propagation delays are usually slowly varying functions of frequency, therefore the received signal at Rx can

be modified as

$$\sum_i a_i(t)x(t-\tau_i(t)). \tag{2.2}$$

Since the channel is linear, it can be described by the response $h(\tau, t)$ at time t to an

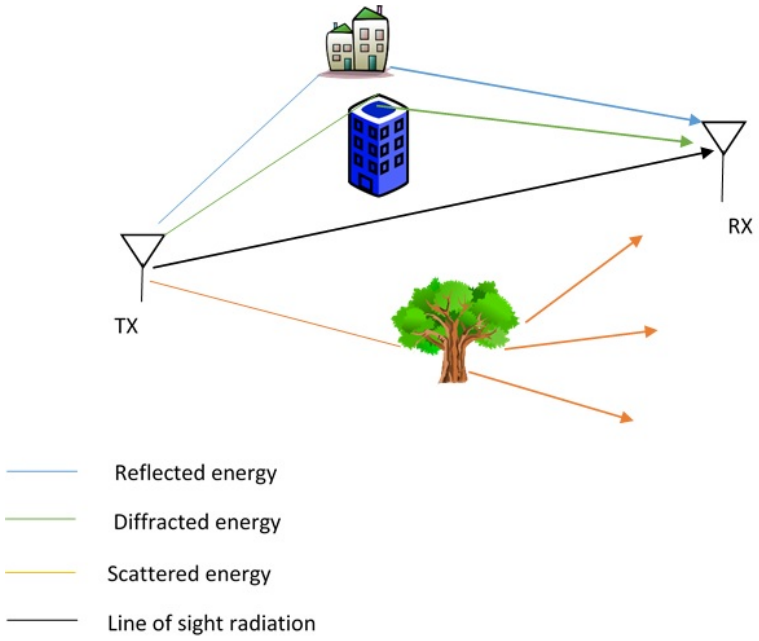

Figure 2.1: Propagation of electromagnetic radiation

impulse transmitted at time $t-\tau$. In terms of $h(\tau, t)$, the input-output relationship can be written as:

$$y(t) = \int_{inf}^{inf} h(\tau, t)x(t-\tau)d\tau. \tag{2.3}$$

After comparing (2.2) with (2.3), it is noted that impulse response can be written as

$$h(\tau, t) = \sum_i a_i(t)\delta(\tau - \tau_i(t)). \tag{2.4}$$

When the Tx and Rx are stationary, the impulse response can be reduced as:

$$h(\tau, t) = \sum_i a_i\delta(\tau - \tau_i). \tag{2.5}$$

Furthermore, a time-varying frequency response can be written as

$$h(f, t) = \sum_i a_i(t)\exp(-j2\pi f\tau_i(t)). \tag{2.6}$$

For a discrete time baseband model, it is assumed that the input waveform is bandlimited to W. According to the sampling theorem, any waveform bandlimited to $W/2$ can be expanded in terms of the orthogonal basis $sinc(Wt-n)_n$, with coefficients given by the samples (taken uniformly at integer multiples of $1/W$), then the equivalent impulse response can be written as

$$h_b(t) = \sum_i a_i^b(m/W)sinc(l-\tau_i(m/W)W), \tag{2.7}$$

where a_i^b is the gain of path ,l is the tap can be interpreted as samples of the low-pass filtered baseband channel response and m is an integer.

2.2.2 Fast and Slow Fading

One of the most important channel parameters is the time-scale of the variation of the channel. How fast do the taps change as a function of time? From the following form of the impulse response

$$h_b(t) = \sum_i a_i^b(m/W)sinc(l-\tau_i(m/W)W) \tag{2.8}$$

$$\sum_i a_i(m/W)\exp(-j2\pi f_c\tau_i(m/W))sinc(l-\tau_i(m/W)W) \tag{2.9}$$

The baseband output is the sum of the delayed replicas of the baseband input over each path. The phase is changed by $\pi/2$ (i.e., is changed significantly) when the delay on the path changes by $1/(4f_c)$, or equivalently, when the path length changes by a quarter wavelength, i.e., by $c/(4f_c)$. If the path length is changing at velocity v, the time required for such a phase change is $c/(4f_cv)$ where doppler shift (D) at frequency f_c is f_cv/c. When the different paths contributing to the l^{th} tap have different Doppler shifts, the magnitude of $h_l[m]$ changes significantly with time-scale inversely proportional to the maximum difference between the Doppler shifts. This maximum difference is called the Doppler spread(D_s) and it can be represented as

$$D_s = \max_{n,k} f_c\left|\tau_n'(t)-\tau_k'(t)\right|, \tag{2.10}$$

where τ_n' and τ_k' are Doppler shifts at paths n and k respectively. The coherence time (T_c) of a wireless channel is the interval over which the channel impulse response changes significantly. T_c can be formulated as

$$T_c = \frac{1}{4D_s}.$$

In wireless communication literature, a channel is classified as fast fading if Tc is much shorter than the delay requirement of the application, and slow fading if Tc is longer.

2.3 Secrecy rate and outage probability

In [69], Shannon put forward a novel conception of information-theoretic security. This model assumed that a private key, K, is used to encrypt the confidential message, M, to yield the cipher, C, which is then transmitted over a noiseless channel. Shannon assumed that the eavesdropper has unbounded computational power, knowledge of the coding scheme sent by the legal transmitter, and access to an identical copy of the received signal at the legal receiver. The formulation of perfect secrecy was defined by requiring that, after a cryptography is intercepted by the eavesdropper, the *a posteriori* probabilities of this cipher representing various messages are identically equal to the *a priori* probabilities of the same messages before the interception. In other words, perfect security requires

$$I(M, C) = 0,$$

where $I(.,.)$ is the mutual information. Furthermore, it was shown that perfect secrecy is possible but requires the number of confidential messages to equal the number of possible keys when the number of confidential messages is finite. Based on the Shannon information-theoretic security, Wyner proved the definition of secrecy capacity [38]. In 6.2, the information signal , X is sent to Bob over the main channel, which is modelled as a discrete memoryless channel. Alice receives Y, which subsequently passes through an additional wiretap channel before being observed by

the eavesdropper, Z. Wyner focused on maximising the transmission rate in the main channel while cancelling the leakage of information to the wiretapper. In particular, Alice has a confidential message, W, which is uniformly distributed over 1, ..., 2^{nR}, where R is the rate of the legal link and n is the block length of this link. The function of the legal transmitter is to send W reliably to the legitimate receiver whilst keeping it secure from the eavesdropper. More specifically, for every $\epsilon > 0$ it is necessary that

$$R_e - \epsilon < \frac{1}{n} H(W|Z^n),$$

where $H(W|Z^n)$ is entropy of W conditioned on Z^n, for large n, where R_e shows the uncertainty of message W at eavesdropper, and it is noted that

$$R - R_e = \frac{1}{n} I(W; Z^n)$$

is the amount of information leaked to the eavesdropper. A message, W, is asymptotically perfectly secure from the eavesdropper [70] if

$$\frac{1}{n} I(W; Z^n) < \epsilon.$$

Recently, secrecy was studied in fading channels, including the use of outage

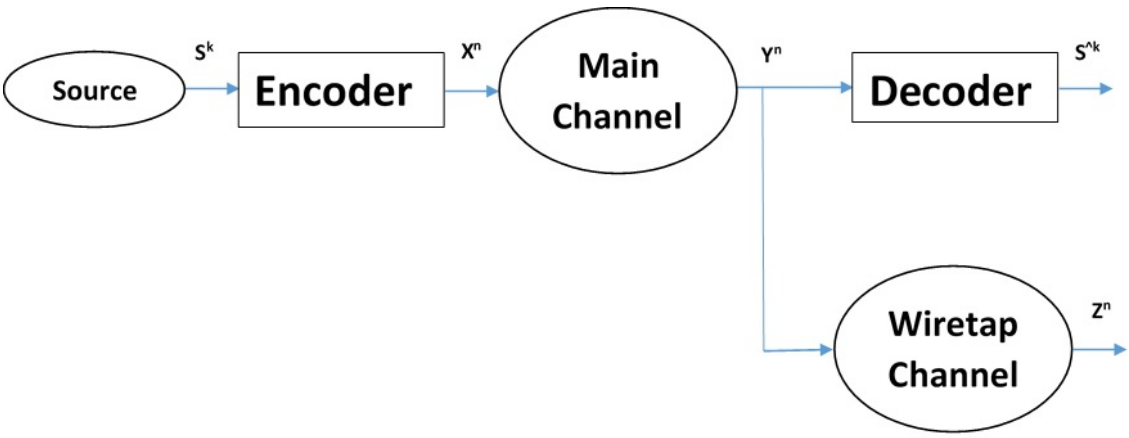

Figure 2.2: Illustration of wiretap channel

.

probability performance metrics. In physical layer security, outage metrics are

presented equivalently to conventional rate outage metrics. For example, the secrecy outage probability (P_O) is the likelihood that the instantaneous secrecy rate (R_s) is below a pre-determined threshold, ζ, for a fading channel distribution [71]:

$$P_O = Prob(R_s < \zeta).$$

Furthermore, the authors in [72] proposed a specific scheme of the Wyner model wherein the legal channel is noiseless and the wiretap channel is a binary symmetric channel. They then analysed the capability of systematic linear codes for preserving the secrecy of the transmitted message. In the case of the degraded wiretap channel with additive Gaussian noise, and C_M and C_W as the Shannon capacities of the legal and wiretap channels [39], the essential result for the secrecy capacity C_S is

$$C_s = C_M - C_W.$$

2.4 Game theory models

Two major game-theoretic approaches can be used to model PHY security in CR:

- Non-cooperative games: Selfish players in non-cooperative games make decisions independently. This does not mean that players do not cooperate, but rather that any cooperation must be self-enforcing. The Nash equilibrium is a well-known solution of non-cooperative game for selfish nodes. The Nash equilibrium is achieved if every player faces a situation in which its present strategy is optimal when other players do not change their strategies. The Stackelberg game is defined as a strategic game in which a player acting as a leader moves first and the other players move afterward, acting as followers. The Stackelberg game is a non-cooperative game and can be solved via a subgame perfect Nash equilibrium.

- Cooperative game: In a cooperative game, players have the ability to create enforceable contracts. The players have a common objective of coalition,

and cooperate to maximise this. In other words, players in a coalition can coordinate strategies and agree on how the total payoff is to be divided among member players. A Nash bargaining game is used to solve cooperative games, wherein the goal of the players is to maximise the product of their gains given what they would gain without cooperation.

Chapter 3

Physical layer security in underlay cognitive radio networks

The open nature of the wireless medium makes it susceptible to malicious eavesdropping, and to counter this vulnerability, many recent studies have focused on the cooperative jamming paradigm. The game-theoretic approach has been recently considered as providing potential solutions for power control in the cognitive radio network (CRN) underlayer. A critical issue in applying game theory is the selection of its proper cost function. In this chapter, cooperative jamming is proposed to enhance primary secrecy rate, and a new chaos-based cost function is introduced in order to design a power control algorithm and analyse the dynamic spectrum-sharing issue in the uplink of cellular CRNs. For secondary users as the game players in underlay scenarios, utility/cost functions are defined, taking into account the interference from and the interference tolerance of the primary users. A proof for the existence of the Nash equilibrium in this power control game is presented, which leads to significantly lower power consumption and a relatively fast convergence rate when compared to existing game algorithms. Simulation results indicate that the primary secrecy rate is significantly improved by cooperative jamming and the proposed power control algorithm achieves low power consumption.

3.1 Introduction

In this chapter, a new scenario is proposed wherein the PU allows the SUs to access its spectrum for better secrecy performance. It is assumed that the eavesdropper ED can intercept the primary transmissions. It is moreover assumed that the SUs are used as multi-antenna jammers for primary transmissions to create interference at the ED. In such networks, a primary user may lease portions of a licensed spectrum to a secondary user in exchange for enhancement of its security performance. This scenario avoids the regulatory issues or monetary transactions that commonly hinder the implementation of the property-rights spectrum leasing concept. Moreover, a new game theory-based algorithm for power control is used to reduce interference in the underlay CRNs. The contributions of this work are summarised as follows:

- A resource allocation scheme (i.e. power) is proposed for spectrum leasing to maximise the primary secrecy rate with perfect knowledge of channel state information (CSI).
- A novel and efficient cost function based on a chaotic logistic map is proposed, which guarantees convergence of the '*power*' game to a unique Nash equilibrium.
- Power control is achieved with a significant reduction in power consumption for cognitive users (by at least half compared to other methods).
- It is also shown that the rate of convergence of the proposed chaotic algorithm is relatively fast compared to existing iterative methods.

3.1.1 System model

In the system model (6.1), a CR spectrum-sharing network includes a set of N cognitive SUs coexisting with the PUs, a primary base station (PBS) (serving the PUs), and a secondary base station (SBS) (serving the cognitive network). Cognitive users take advantage of the coexistence scenario to share spectrum resources with

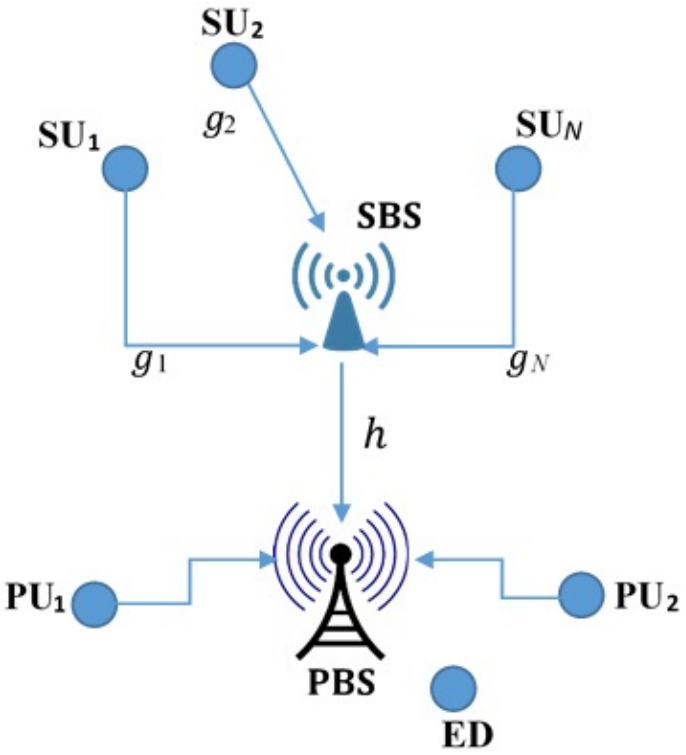

Figure 3.1: Illustration of an uplink CR system model with N SUs and 2 PUs

primary users. Let g_i and h_i denote the link gains from the cognitive user i to the SBS and the PBS, respectively. It is proposed that the PUs, SUs, and the ED have single antennae. In general, the secrecy rate R_{sec} is defined as:

$$R_{sec} = (R_D - R_E)^+ \tag{3.1}$$

where R_D and R_E are the information rates at the destination and eavesdropper, respectively, and $(x)^+ = \max(0, x)$ refers to the positivity value of the secrecy rate. For convenience, the $(\cdot)^+$ sign is omitted from subsequent calculations. Two phases are proposed:

1) Phase 1: The cognitive SBS can play the role of a multiple-antenna jammer with N antennas when N SUs send a jamming signal through the SBS. The received signal at the PU is

$$x_P = \sqrt{P_p} h_{pp} s + \sqrt{P_s} \mathbf{h}_{sp} \mathbf{v} z + n_P, \tag{3.2}$$

where s is the primary message signal from the PU with transmission power P_p, z is the jamming signal, $\mathbf{v}$ is the pre coding weighting vector for z, P_s is the secondary power, $h_{pp} \sim \mathcal{N}(0, \sigma_h^2)$ is the channel coefficient between the PU and PBS, $\mathbf{h}_{sp} \sim \mathcal{N}(\mathbf{0}_N, d_{s,p}^{-\beta}\mathbf{I}_N)$ is the channel vector between the SBS and PU (of length N due to N multiple transmit antennas at the SBS), $n_P \sim \mathcal{N}(0, \sigma^2)$, β is the pass loss exponent, and $d_{s,p}$ is the distance between the SBS and PU. The received signal at the ED in Phase 1 is

$$x_{ED} = \sqrt{P_p} h_{pe} s + \sqrt{P_s} \mathbf{h}_{se} \mathbf{v} z + n_{ED}, \tag{3.3}$$

where $h_{pe} \sim \mathcal{N}(0, \sigma_h^2)$ is the channel coefficient between the PBS and ED, $\mathbf{h}_{se} \sim \mathcal{N}(\mathbf{0}_K, d_{S,E}^{-\beta}\mathbf{I}_K)$ is the channel vector between the SBS and the ED, and the distance between them is $d_{S,E}$. The information rate at PU is then

$$R_P = \log_2 \left(1 + \frac{P_p \left| h_{pp} \right|^2}{\sigma^2 + P_s \left| (\mathbf{h}_{sp})^\dagger \mathbf{v} \right|} \right). \tag{3.4}$$

Simultaneously, the leakage rate at the ED is

$$R_{ED} = \log_2 \left(1 + \frac{P_p \left| h_{pe} \right|^2}{\sigma^2 + P_s \left| (\mathbf{h}_{se})^\dagger \mathbf{v} \right|} \right). \tag{3.5}$$

According to (C.3), the achievable primary secrecy rate (PSR), denoted by R_S, can be obtained as follows:

$$\begin{aligned} R_{SEC} &= R_P - R_{ED} \\ &= \log_2 \left(1 + \frac{P_p \left| h_{pp} \right|^2}{\sigma^2 + P_s \left| (\mathbf{h}_{sp})^\dagger \mathbf{V} \mathbf{h}_{sp} \right|} \right) \\ &\quad - \log_2 \left(1 + \frac{P_p \left| h_{pe} \right|^2}{\sigma^2 + P_s \left| (\mathbf{h}_{se})^\dagger \mathbf{v} \right|} \right). \end{aligned} \tag{3.6}$$

2) Phase 2: The N cognitive SUs communicate through the SBS with limited transmitted power to reduce interference with primary transmissions. The received signal at the ith SU is

$$x_{s,i} = \sqrt{P_p} h_{ps,i} s + \sqrt{p_i} g_i s_i' + \sum_{j=1, j \neq i}^{N} \sqrt{p_j} q_{i,j} z_j' + n_{s,i}, \tag{3.7}$$

where s_i' and z_j' are the secondary signal with transmitted power p_i and p_j, respectively, $h_{ps,i} \sim \mathcal{N}(0, \sigma_h^2)$ is the channel coefficient between the PU and the ith SU, $g_i \sim \mathcal{N}(0, \sigma_h^2)$ is the channel coefficient between the ith SU and the SBS, $q_i \sim \mathcal{N}(0, \sigma_h^2)$ is the channel coefficient between the ith SU and jth SU, and $n_{s,i} \sim \mathcal{N}(0, \sigma^2)$. The rate at the ith SU is

$$R_s = \log_2 \left(1 + \frac{p_i \left| g_i \right|^2}{\sum_{j=1, i \neq j}^{N} p_j \left| q_{i,j} \right|^2 + \mu_i + \sigma^2} \right), \tag{3.8}$$

where μ_i is the interference power from the PUs affecting the ith SU signal at the SBS.

3.2 Phase I: Enhancing the primary secrecy rate

It is assumed that the SU and PU have global instantaneous CSI information and that the SBS has knowledge of the CSI to the ED when the ED is active. A power weight vector can be designed for the SBS to maximize the interference with the ED, while minimising the interference with the PU. The solution of the weight vector for Phase I transmission is given by

$$\begin{aligned} \mathbf{v}^* = \arg\max & \left| \left(\mathbf{h}_{se} \right)^\dagger \mathbf{V} \mathbf{h}_{se} \right| \\ \text{s.t.} \quad & \left| \left(\mathbf{h}_{sp} \right)^\dagger \mathbf{V} \mathbf{h}_{sp} \right| = 0, \\ & \left| \mathbf{v} \left(\mathbf{v} \right)^\dagger \right| = 1. \end{aligned} \tag{3.9}$$

Using projection matrix theory to provide the solution of optimisation problem in (C.4), $\left| \mathbf{v}_j'^* \right|$ can be achieved as follows:

$$\left| \mathbf{v}^* \right| = \frac{(\mathbf{I} - \mathbf{h}_{sp} (\mathbf{h}_{sp} {\mathbf{h}_{sp}}^\dagger)^{-1} {\mathbf{h}_{sp}}^\dagger) \mathbf{h}_{se}}{\left| (\mathbf{I} - \mathbf{h}_{sp} (\mathbf{h}_{sp} {\mathbf{h}_{sp}}^\dagger)^{-1} {\mathbf{h}_{sp}}^\dagger) \mathbf{h}^{(se)} \right|}, \tag{3.10}$$

where $\mathbf{V} = \mathbf{v}\mathbf{v}^\dagger$. According to (C.5), the achievable primary secrecy rate can be written as

$$R_{SEC} \;=\; \log_2 \left(1 + \frac{P_p \left| h_{pp} \right|^2}{\sigma^2} \right)$$

$$-\log_2\left(1+\frac{P_p\left|h_{pe}\right|^2}{\sigma^2+P_s\left|\left(\mathbf{h}_{se}\right)^{\dagger}\mathbf{v}\right|}\right). \tag{3.11}$$

3.3 Phase II: The power control

Game theory, a strong tool in economics, can also be applied to solve the problem of power control in wireless communication systems [1]. Based on a suitable utility or cost function, the game solution can help to obtain power control policies through effective iterative algorithms In this section, as several SUs will interfere with the PUs to a certain degree, the goal of power control is to limit the power of the SUs and thereby avoid excessive interference. One of the design goals for power control in wireless networks is to ensure that no mobile's SINR falls below its threshold γ_{tar}, to ensure adequate QoS. In this section, a flat fading channel is assumed, with channel gains remaining quasi-static over time. It is assumed that CSI knowledge between the PUs and the SUs is present. The SINR of the ith SU signal received at the SBS is defined as

$$\gamma_i = \frac{p_i g_i}{\sum_{i\neq j} p_j q_{i,j} + \mu_i + \sigma_i^2} \tag{3.12}$$

where

$$\gamma_i \geqslant \gamma_{tar} \quad \forall i, \tag{3.13}$$

and σ_i^2 is the background noise, μ_i is the interference power from the PUs affecting the ith SU signal at the SBS, p_i is the power level of the ith SU, and $q_{i,j} = g_{\mathrm{j}}\delta_{i,j}$. Here, $\delta_{i,j}$ denotes the correlation between the ith SU's signal and the jth SU's signal. Thus, q_{ij} can be seen as an effective link gain from the jth user to the SBS when considering its interference with the ith SU's signal.

In order to meet the user's QoS in CRNs, the power of the ith SU (p_i) should satisfy

$$\sum_{i=1}^{N} p_i h_i \leq T_{max}, \tag{3.14}$$

where T_{max} is the interference tolerance of PUs. However, a cognitive user should reach the minimum required SINR once the network allows it to communicate.

3.3.1 Game theory and problem formulation

To enhance the communication effect, a cognitive user must increase its SINR, which will frequently require high power. However, lower power is useful to decrease interference with other SUs. Therefore, low power and high SINR contradict each other. To resolve the conflict and maximise the benefit of SUs, game theory is applied. Under the assumption that every SU is rational and wants to maximise its benefit, this problem is converted to a non-cooperative game problem. In this section, the SINR-based power control problem is formulated as a non-cooperative game by choosing an appropriate cost function and finding the corresponding Nash equilibrium power vector. The power control game is defined as: $\mathcal{G} = [\mathcal{N},\ \mathcal{P},\ J]$, where now $\mathcal{N}$ is the set of N players (SUs), $\mathcal{P}$ is the strategy (power) set for the SUs, and J is the set of cost functions. The cost function of the ith SU is denoted by $J(p_i, \gamma_i(\mathbf{p}))$, where $\mathbf{p} = [p_1, p_2, \cdots, p_N]$ [3]. The generalised Nash equilibrium problem—in which each player selfishly optimises his own well-being within his strategy set, which also depends on the strategies of the other players—is defined as:

$$\mathcal{G} : \min\ J(p_i, \gamma_i(\mathbf{p})), \quad \forall i = 1, 2, \ldots, N \tag{3.15a}$$

$$\text{s.t.} \quad \sum_{i=1}^{N} p_i h_i \leq T_{max}, \tag{3.15b}$$

$$\gamma_i(\mathbf{p}) \geqslant \gamma_{tar}. \tag{3.15c}$$

The corresponding Nash equilibrium strategy is represented by the power vector $\mathbf{p}^* = [p_1^*, p_2^*, \cdots, p_N^*]$, where p_i^* is the Nash power, with the property that no individual user can lower its cost by deviating from p_i^*, i.e,

$$J(p_i^*, \gamma_i(\mathbf{p}^*)) \leq J(p_i,\ \gamma_i(\mathbf{p}_i^*). \tag{3.16}$$

Here, $\mathbf{p}_i^* = [p_1^*, p_2^*, \cdots, p_{i-1}^*, p_i, p_{i+1}^*, \cdots, p_N^*]$. Every player (i.e., cognitive user) faces a situation in which its present strategy is optimal when other players do not change their strategies; that is, the game achieves the Nash equilibrium. Thus, our power

control algorithm will search for the Nash equilibrium point (i.e., transmitting power level) to maximise the user's utility (i.e., the rate of transmission of information). Note that there are two conflicting objectives. Generally, a higher SINR is targeted for better service. However, a higher SINR is achieved at the cost of increased drain on the battery and higher interference with signals of other users. Therefore, a cost function is defined for each user depending on both power and SINR. In particular, the cost of the difference between the actual SINR and the target SINR, which is chosen based on the estimated frame error rate, is considered. In order to ensure non-negativity and convexity of the cost function (i.e., to allow the existence of a non-negative minimum), the squared SINR error term is used. Furthermore, the basic idea of chaotic optimisation is to map the chaotic variable onto an optimised variable space, and then search for the global optimum using the ergodicity of its chaotic movement [4]. Hence, the chaotic variable is included in the cost function to reduce power consumption to an acceptable level. Based on the SINR constraint in Equation (3.13), the following cost function is constructed:

$$J(p_i, \gamma_i) = ap_i^2 + 2\Delta_{tar,i}\gamma_i + c(\gamma_{tar} - \gamma_i)^2, \tag{3.17}$$

where a and c are constants; $\Delta_{tar,i}$ is an acceptable error level of the target SINR, which is controlled by a chaotic variable to allow a trade-off between p_i and γ_i. For any non-negative a and c, $J(p_i, \gamma_i)$ is a convex function with respect to p_i. Therefore, Nash equilibrium for our power control problem always exists. In order to derive this Nash equilibrium, the partial derivative $\partial J/\partial p_i$, is set equal to zero. Rearranging terms yields

$$\frac{\partial J}{\partial p_i} = 2ap_i + 2\Delta_{tar,i}\frac{g_i}{I_i} + 2c(\gamma_{tar} - \gamma_i)(-\frac{g_i}{I_i}) = 0,$$

where $I_i = \sum_{i \neq j} p_j q_{ij} + \mu_i + \sigma_i$. Substituting $I_i/g_i = p_i/\gamma_i$ yields

$$\gamma_i = (\gamma_{tar} - \Delta_{tar,i}) - \frac{ap_i^2}{c\gamma_i}, \tag{3.18}$$

$$\Rightarrow p_i = (\gamma_{tar} - \Delta_{tar,i})\frac{p_i}{\gamma_i} - \frac{ap_i^2}{c\gamma_i}(\frac{p_i}{\gamma_i}). \tag{3.19}$$

Equation (3.19) can be used to obtain p_i^* through iterations as follows:

$$p_i^{(l+1)} = (\gamma_{tar} - \Delta_{tar,i}^{(l)})\frac{p_i^{(l)}}{\gamma_i^{(l)}} - \frac{a(p_i^{(l)})^3}{c(\gamma_i^{(l)})^2} \triangleq f(p_i^{(l)}), \tag{3.20}$$

where superscript $(\cdot)^{(l)}$ denotes the lth iteration and $\Delta_{tar,i}^{(l)}$ is updated by a logistic map with chaotic variable $ch_i^{(l)}$:

$$ch_i^{(l+1)} = 4ch_i^{(l)}(1 - ch_i^{(l)}), \tag{3.21}$$

$$\Delta_{tar,i}^{(l+1)} = (\gamma_{tar} - \epsilon\gamma_{tar})ch_i^{(l+1)}. \tag{3.22}$$

Here, ϵ is a parameter with a value close to 1 ($\epsilon \in [0.97, 0.99]$ is chosen in this design, i.e., a drift of 1% to 3% from the target SINR γ_{tar} is acceptable), while the initial $ch_i^{(0)}$ has a value chosen in [0, 1].

3.3.2 Convergence to the unique Nash equilibrium

Because a Nash equilibrium is a fixed point of the best response functions, the existence of at least one Nash equilibrium point is guaranteed by a proper choice for the cost function in Equation (5). If a fixed point of the algorithm, $p_i^{(l+1)} = f(p_i^{(l)})$, exists, and if the function f satisfies three properties—positivity, monotonicity, and scalability—then the power control algorithm will converge to a unique Nash equilibrium. In the following, it will be proved here that these three properties are satisfied in our proposed algorithm:

1) *Positivity:* $f(p_i) > 0$. This is easily obtained from Equation (3.20) based on the fact that $a/c \ll 1$ can be chosen and the fact that $\gamma_{tar} \gg \Delta_{tar,i}$, as seen from Equation (3.22).

2) *Monotonicity:* $p_i > p_i'$ then $f(p_i) > f(p_i')$. To prove this property, the term $f_i(p) - f_i(p')$ is considered, which is equal to

$$\frac{\gamma_{tar} - \Delta_{tar,i}}{g_i}(I_i - I_i') - \frac{a}{cg_i^2}(p_i I_i^2 - p_i' I_i'^2).$$

Since $p_i > p_i'$, it holds that $I_i > I_i'$. Also, it has been assumed that $a/c \ll 1$, and hence $a/(cg_i^2) \ll (\gamma_{tar} - \Delta_{tar,i})/g_i$. Thus, $f_i(p_i) - f_i(p_i')$ has a positive value.

3) *Scalability:* $f(\alpha p_i) < \alpha f(p_i)\ \forall\ \alpha > 1$. If this condition is satisfied, the algorithm converges to a unique fixed point. From Equation (3.20), it can be found that

$$\alpha f(p_i) - f(\alpha p_i) = \frac{a p_i^3}{c\gamma^2}(\alpha^3 - \alpha). \tag{3.23}$$

It is evident from Equation (4.6) that the *scalability* condition is satisfied due to $\alpha > 1$.

Positivity and monotonicity of $f(p_i)$ impose constraints on acceptable values of I_i, but scalability restricts the noise power level allowed for the receiver and generates a limit less than that required for monotonicity.

3.3.3 Iterative chaos-based power control algorithm

The procedure for applying a chaotic iterative algorithm for power control is as follows:

1. *Step 1*: Set the target SINR, γ_{tar}, and the interference tolerance of PUs, T_{max}. Also, obtain the channel matrix with coefficients g_i and q_{ij}. Set the initial value $ch_i^{(0)}$ in [0,1]. Set $l = 0$.

2. *Step 2*: Increase $l = l + 1$. Compute $ch_i^{(l)}$ and $\Delta_{tar,i}^{(l)}$ by using Equation (3.21) and Equation (3.22), respectively.

3. *Step 3*: Apply Equation (3.20) to calculate $p_i^{(l)}$ and then compute SINR ($\gamma_i^{(l)}$) according to Equation (1).

4. *Step 4*: If $\gamma_i^{(l)} < \epsilon\gamma_{tar}$ then return to Step 2. Otherwise, stop the chaotic search by taking $ch_i^{(l+1)} = ch_i^{(l)}$ and then take $\Delta_{tar,i}^{(l+1)} = \Delta_{tar,i}^{(l)}$ and $p_i^{(l+1)} = p_i^{(l)}$.

3.4 Results and discussion

In this section, the following two cases are used to highlight the effect of the jammer and interference on the secrecy rate and quality of service, respectively, in cognitive radio:

i) Case I: Primary secrecy rate. In this case, the locations of the two PUs, PBS, and SBS are fixed at the coordinates (0,0.3), (0,0.5), (0,1), and (0,0), respectively. To highlight the effect of eavesdropper position on the secrecy rate, two schemes are considered depending on locations of eavesdropper as follows: Location I (0,0.5), Location II (0,1.3) and Location III (1.2,0). It is assumed that the path loss model $h = d^{-\alpha}$ is used with path loss exponent $\alpha = 3.0$. Distances are in units of Km.

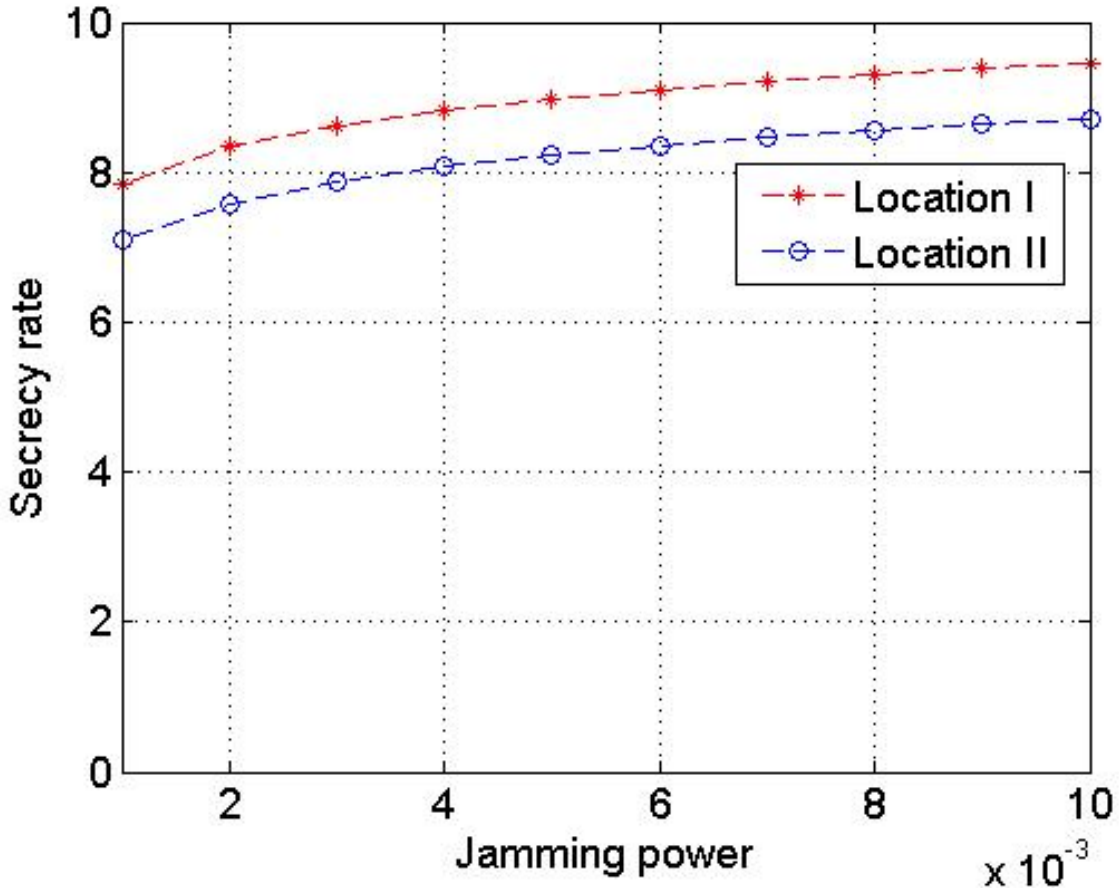

Figure 3.2: Secrecy rate vs. jamming power

Figure 4.13 shows the effect of the jamming power of SUs on the primary secrecy rate with regard to position of the eavesdropper. The secrecy rate increases significantly with jamming power due to the increase of interference with the

eavesdropper and the orthogonality in Equation (C.5). It can also be concluded that the secrecy rate is increased when the eavesdropper is located farther from the legitimate transmitter, due to the decrease of h_{pe}.

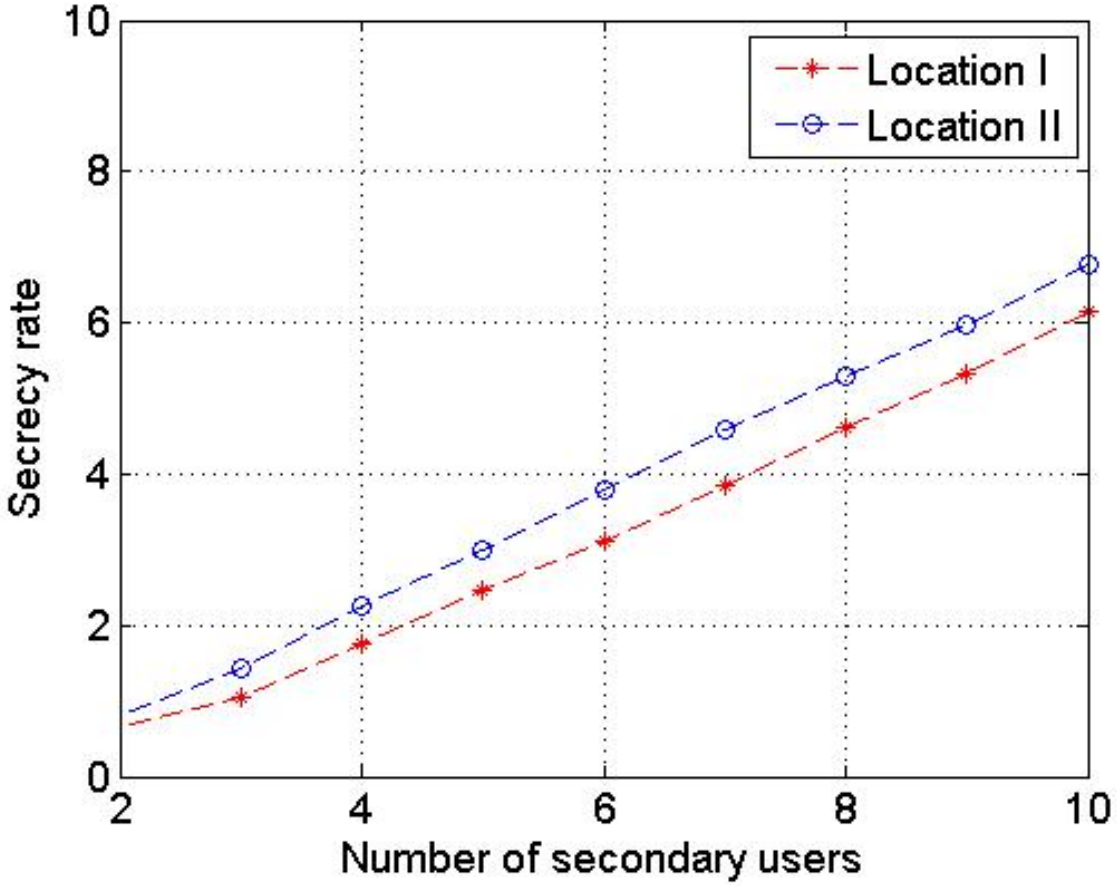

Figure 3.3: Secrecy rate vs. number of SUs

Figure 3.3 plots the effect of the number of SUs on the primary secrecy rate with regard to position of eavesdropper. The secrecy rate increases significantly with the number of SUs, due to the increasing interference with the eavesdropper.

i) Case II: Interference in an underlay cognitive radio network. In this study, three different underlay scenarios are considered to study the effects of interference of PUs on the cognitive users while the interference tolerance of PUs is preserved (all three scenarios use 2 PUs): i) Scenario 1: three SUs; ii) Scenario 2:

five SUs; and iii) Scenario 3: ten SUs. The channel coefficient matrix, $\mathbf{G}$, for each scenario is generated based on the on the locations of the PUs and SUs with respect to the base stations and the cross correlation between user signals. In particular, the channel gain, g_i, is generated by the attenuation model $g_i = A/d^n$, where d is the distance between the user and the base station, which is uniformly randomly generated. Here, $\{A,\ n\} = \{10^{-4},\ 3.5\}$ for Scenario 2 and $\{10^{-8},\ 4\}$ for Scenario 3. However, in Scenario 1, the same fixed-channel model as in [3] is used for comparison purposes. In this case, the channel matrix is

$$\mathbf{G} = \begin{pmatrix} 1 & 0.0882 & 0.0375 \\ 0.1524 & 0.95 & 0.3501 \\ 0.0767 & 0.0244 & 0.99 \end{pmatrix}. \tag{3.24}$$

A comparison is carried out between the proposed system with existing algorithms. These are the revised Nash algorithm [1, 5] (see (3.25)), power balancing by Koskie and Gajic (KG) [3] (see Equation (3.26)), and the revised KG [7, 9] (see Equation (3.27)). Their iterative algorithms are as follows:

$$p_i^{(l+1)} = (\gamma_{tar})\frac{p_i^{(l)}}{\gamma_i^{(l)}} + \frac{a(T_{max} - p_i^{(l)})}{c} \tag{3.25}$$

$$p_i^{(l+1)} = (\gamma_{tar})\frac{p_i^{(l)}}{\gamma_i^{(l)}} - (\frac{a{p_i^{(l)}}^2}{c{\gamma_i^{(l)}}^2}) \tag{3.26}$$

$$p_i^{(l+1)} = (\gamma_{tar})\frac{p_i^{(l)}}{\gamma_i^{(l)}} - \frac{p_i^{(l)}}{\gamma_i^{(l)}}\sinh^{-1}(\frac{a{p_i^{(l)}}^2}{c{\gamma_i^{(l)}}^2}), \tag{3.27}$$

respectively, with $a/c = 0.25$ for all algorithms. As the KG and revised KG algorithms are similar approaches, only the results of the revised KG algorithm are displayed here. The system parameters are set as follows: $\gamma_{tar} = 5$ in both scenarios; $T_{max} = 35mW,\ \epsilon = 0.99$ for Scenario 1, and $T_{max} = 3.5mW,\ \epsilon = 0.98$ for Scenarios 2 and 3.

Figure 3.4 shows the comparison of average power consumption across 3 SUs in Scenario 1. It is clear that the power consumption of the proposed algorithm is less than that of the revised KG algorithm and particularly the revised Nash algorithm.

In addition, the proposed algorithm converges near 55 iterations, much faster than the revised KG algorithm (after 450 iterations) and only slightly slower than the revised Nash algorithm (after 15 iterations). Figures 3.5 and 3.6 show the same

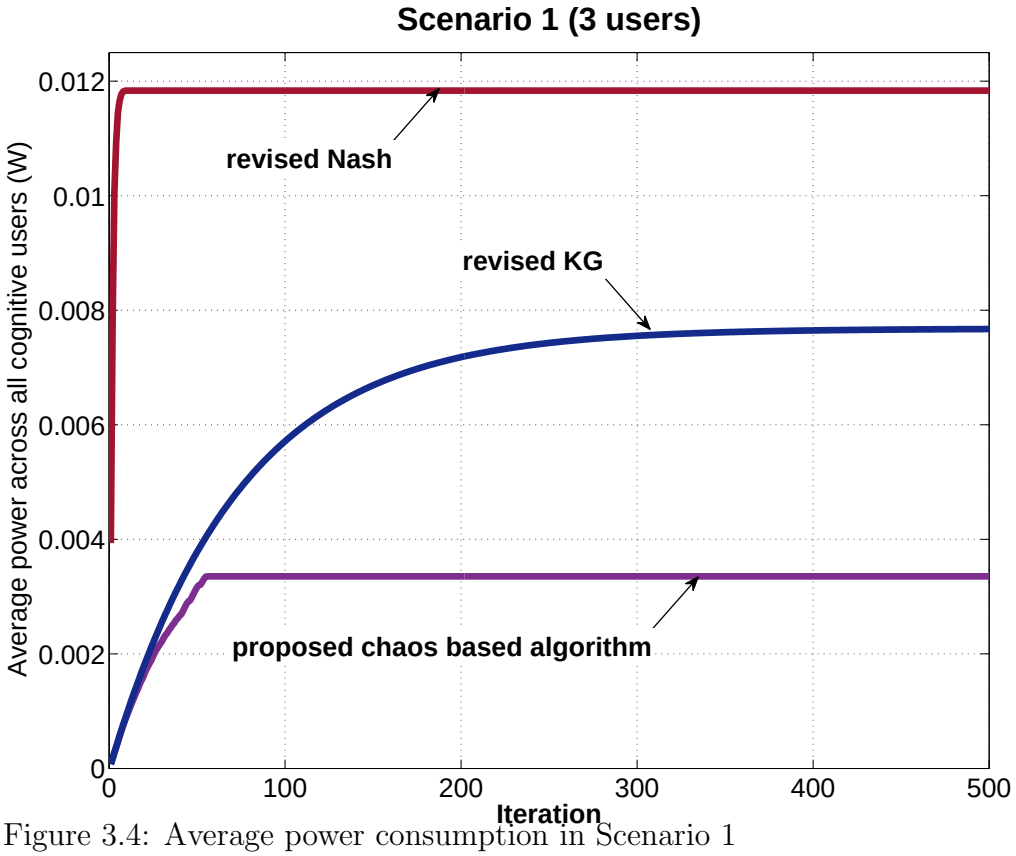

Figure 3.4: Average power consumption in Scenario 1

performance behaviour with more cognitive users (5 SUs and 10 SUs, respectively) in Scenarios 2 and 3. However, in these scenarios, the convergence rate tends to be faster for all algorithms when more users are involved.

As the proposed algorithm is applied in an underlay scenario, it is necessary to study the effect of variation in the interference between PUs and SUs. Figure 3.7 shows the impact of the interference from the PUs on the average SINR across the cognitive users. When the interference level increases, it is expected that the SINR will be reduced. However, the SINR of the proposed chaos-based algorithm changes

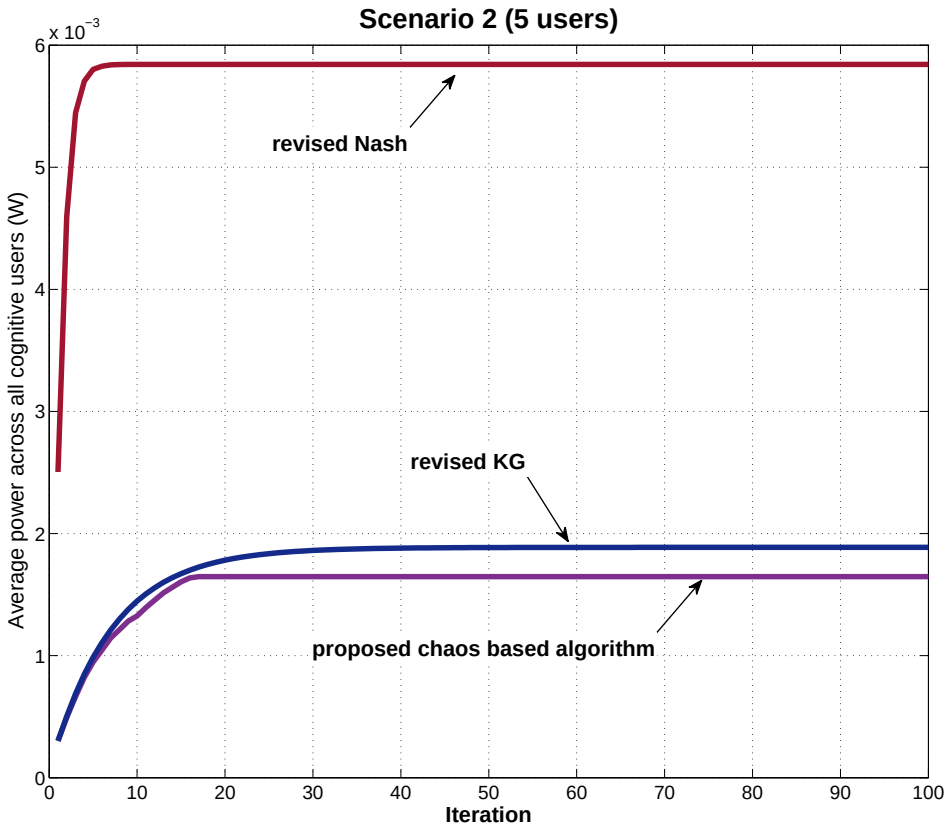

Figure 3.5: Average power consumption in Scenario 2

more slowly (that is, it remains almost stable under the changing interference environment) compared with the other two algorithms. In addition, although the SINR of the proposed algorithm is slightly smaller than that of the revised KG algorithm, it is generally significantly better than the revised Nash approach.

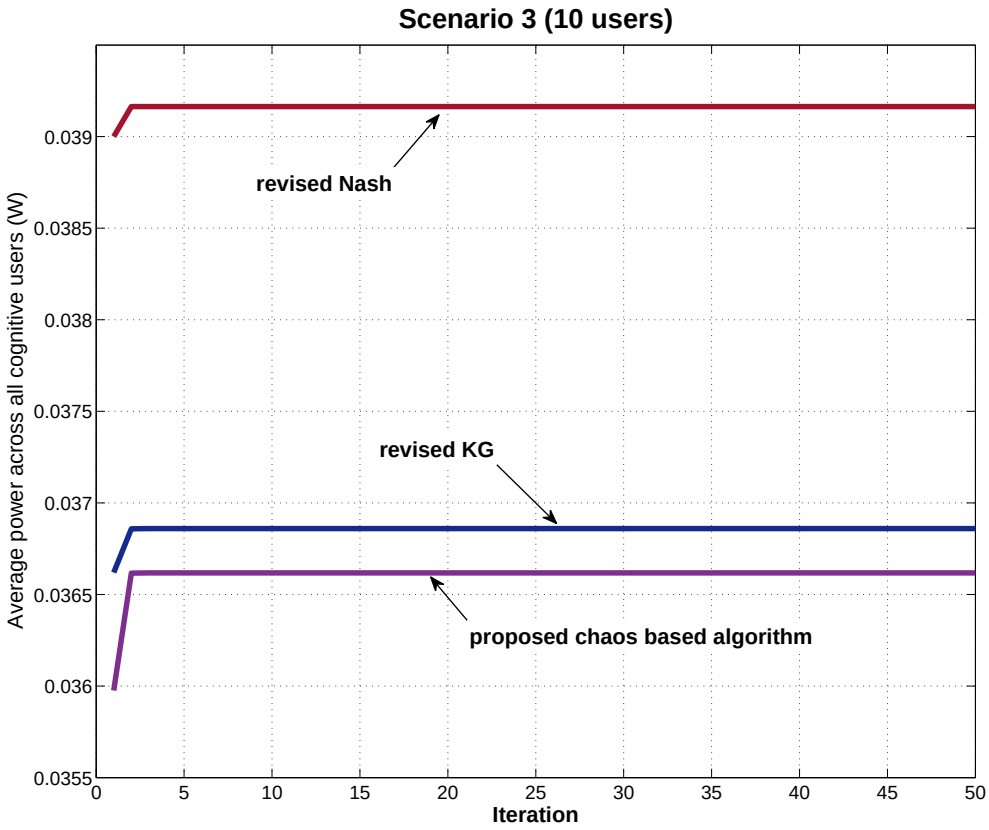

Figure 3.6: Average power consumption in Scenario 3

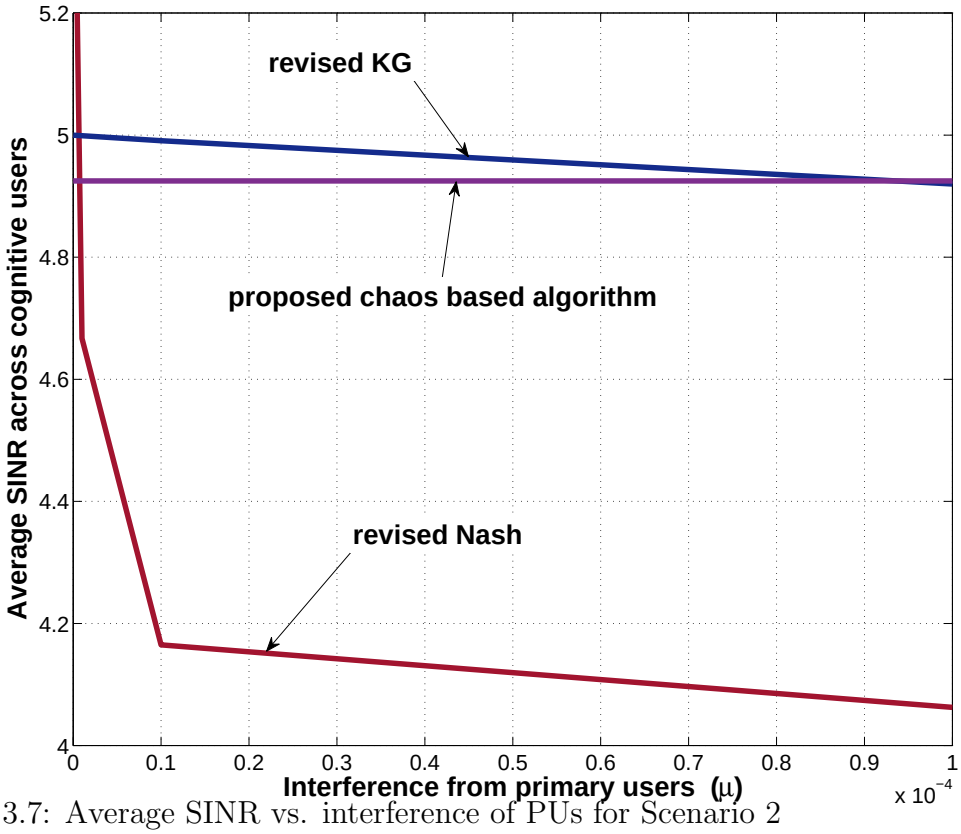

Figure 3.7: Average SINR vs. interference of PUs for Scenario 2

3.5 Conclusions

In this chapter, cooperative jamming has been proposed to maximise the primary secrecy rate and achieve a sustainable secondary quality of service in underlay CRNS. A novel chaotic cost function for power control, based on a non-cooperative game among SUs, has been proposed for CRNs. A resultant Nash equilibrium has been achieved and shown to be unique in the coexistence scenario of PUs and SUs in CR systems. The simulation results indicate that the achievable primary secrecy rate is significantly enhanced by our cooperative jamming algorithm. In addition, the numerical results show that the proposed algorithm achieves lowest power consumption at the expense of a small drift (1-3%) from the target SINR in comparison with existing game algorithms, whilst having a relatively fast convergence rate.

Chapter 4

Physical layer security in cognitive radio networks via chaotic OFDM

Cognitive radio (CR) holds enormous potential for improving spectral utilisation, making it important and challenging to design a CR network with an adaptive access system and address its physical layer security issues. Secondary transmitters usually transmit over multiple non-contiguous frequency holes, and hence a multicarrier-based system is one of the best candidates for CR networks design. This chapter proposes an integrated scheme with chaotic scrambling (CS), chaotic artificial noise, and a chaotic shift keying (CSK) scheme in an orthogonal frequency division multiplexing (OFDM)-based CR system to enhance its physical layer security. By employing the chaos-based third-order Chebyshev map to achieve the optimum bit error rate (BER) performance of CSK modulation, the proposed three-layer integrated scheme outperforms the traditional OFDM system in an overlay scenario with a Rayleigh fading channel. Importantly, under three layers of encryption that is based on chaotic scrambling, chaotic artificial noise, and CSK modulation, a large key size can be generated to resist brute-force attacks and eavesdropping, leading to a significantly improved security rate.

4.1 Introduction

In this chapter, a security mechanism for OFDM-based CR networks. This mechanism provides extreme sensitivity to initial conditions in generating the chaotic sequence. A slight difference in the initial condition of the chaotic sequences between transmitter and receiver results in an almost completely different position matrix, leading to failure in decrypting the data signal and thereby guaranteeing the security of the system. The Chebyshev map is selected to generate a chaotic reference sequence in CSK, as this map satisfies the necessary conditions for optimum BER in this proposed chaotic OFDM (C-OFDM) scheme. The feasibility of employing three layers of security is investigated as follows:

1. *Layer 1*: The constellation symbols are dynamically scrambled using a scrambling matrix, which is generated based on the mixing property of the chaotic dynamical systems (using a chaos-based logistic map).

2. *Layer 2*: The third-order Chebyshev map is used to perform CSK modulation, which allows spreading of each frame of the scrambled data with a specific initial condition.

3. *Layer 3*: This is introduced by adding chaotic artificial noise to enhance the secrecy rate.

Our contributions are the following:

1. Three-layer protection is proposed for CR networks. The first and second layers provide protection against brute-force attacks, while the third layer provides protection against eavesdroppers.

2. The secrecy rate and the power allocation of the proposed C-OFDM CR networks are optimised under different scenarios for eavesdroppers.

   (a) *Scenario I – Single eavesdropper:* An efficient optimisation scheme is provided to maximise the secondary secrecy rate (SSR) under the flat

fading channel model. Subsequently, the secondary power optimisation allocation problem is analysed and solved at the secondary transmitter (ST).

(b) *Scenario II – Multiple eavesdroppers:* Analysis is provided for the proposed CR systems under the malicious attempt of multiple non-colluding eavesdroppers that are distributed according to a homogeneous Poisson point process (PPP) distribution around secondary transceivers. This is to highlight the impact of multiple eavesdroppers on the primary secrecy rate (PSR) and SSR. It is shown that the secrecy outage probability and the mean secrecy rate achieved for CR systems under the non-colluding eavesdroppers are significantly lower than under traditional transceivers without artificial noise.

4.2 System model and architecture of security layers

The proposed CR network architecture is shown in Figure 4.1 with two primary users, two secondary (unlicensed) users, and a primary (licensed) base-station. The primary users have a license to operate in a certain spectrum band, whilst the primary base-station is a fixed infrastructure network component, which has a spectrum license, such as base-station transceiver system (BTS) in a cellular system.

To improve physical layer security in CR networks, three layers of security are proposed, which are applied to each frame of plain data (Figure 4.2) utilising chaotic scrambling, chaotic modulation, and artificial noise. The first and second layers are important for improving physical security against brute force attacks, while the third layer is useful to enhance secrecy rates against eavesdroppers. The goal of jamming the signal/artificial noise is to create confusion at the eavesdroppers in order to reduce their information rate. Notice that the legitimate receiver has *a priori* knowledge of the jamming signal sent by the source. This can be implemented

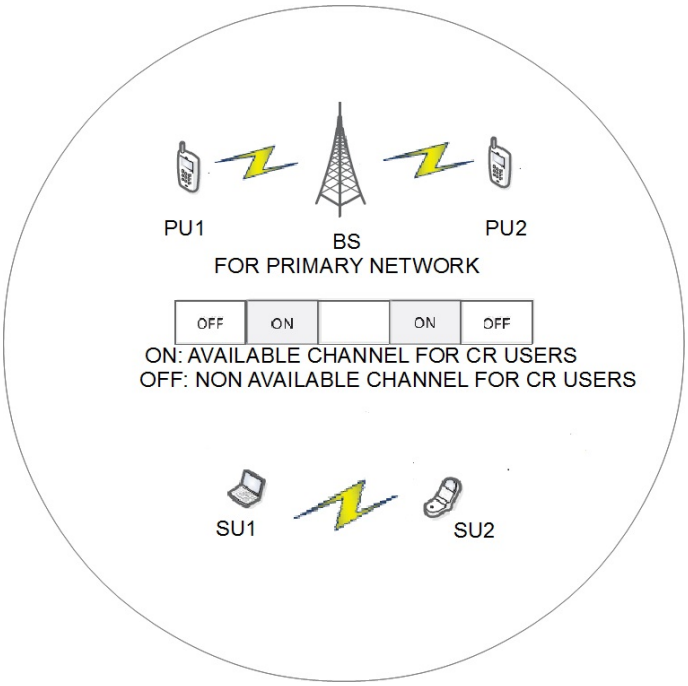

Figure 4.1: Cognitive radio architecture

in practice with a small amount of overhead. For example, the jamming signal can be Gaussian noise generated by a chaotic pseudo-random generator with finite states, and the trusted nodes maintain the same pseudo-random generator. Only the state of the pseudo-random generator needs to be sent to the destination via a separate and secure control channel. In this way, the legitimate receivers have complete knowledge of the jamming signals.

4.2.1 Transmitter

OFDM-CSK with a discrete chaotic sequence for modulation is considered in the system, with respect to the non-coherent advantages of DCSK and the spectral efficiency of multi-carrier modulation. For mathematical simplification, a mathematical model is described for a single user only. As shown in Figure 4.3, for each user, a chaotic code is generated and used as a reference and spreading code. The input information sequence is first converted into U parallel data sequences

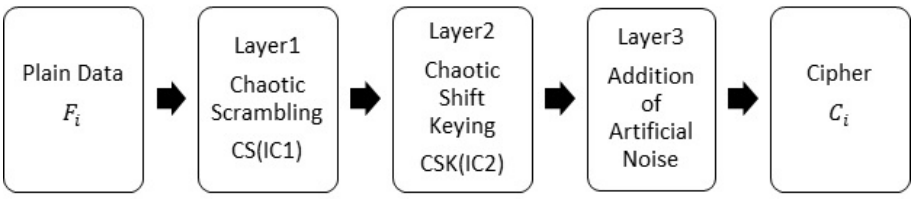

Figure 4.2: Three layers of security

with each bit being of equal probability of +1 and -1.

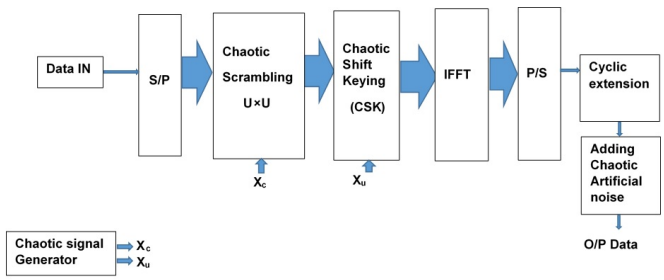

Figure 4.3: Block diagram of the OFDM-CSK transmitter

Let $\mathbf{S}$ be the $U \times U$ scrambling matrix, which is obtained by the logistic map-based chaotic sequence $\mathbf{x}_c$, generated from the chaotic signal generator. Also let $\mathbf{s} = [s_1,\ s_2, \cdots, s_U]^T$ and $\mathbf{e} = [e_1,\ e_2, \cdots, e_U]^T$ represent the data vectors before and after scrambling (the first layer of security), respectively. It holds that

$$\mathbf{e} = \mathbf{s} \times \mathbf{S}. \tag{4.1}$$

The u^{th} sub-stream is spread with the chaotic spreading code $\mathbf{a}_u = [a_{u,1},\ a_{u,2}, \cdots, a_{u,\beta}]$ (generated by the same chaotic signal generator) through the chaotic reference signal

$$x_u(t) = \sum_{k=1}^{\beta} a_{u,k} h(t - kT_c), \tag{4.2}$$

where $h(t)$ is the square-root-raised-cosine filter, $\beta$is the length of chaotic spreading code and T_c is the chip duration. This filter is band-limited and is normalised to have unit energy. Let $H(f) = F(h(t))$, where F denotes the Fourier transform. It is assumed that $H(f)$ is limited to $[-B_c/2,\ B_c/2]$, which satisfies the Nyquist criterion with a roll-off factor α $(0 < \alpha < 1)$. Here, $B_c = (1+\alpha)/T_c$. Note that the first two subcarriers are used to modulate the reference signals $x_u(t)$ and $x_c(t)$. The remaining subcarriers are used to carry data. Therefore, the transmitted signal of the single-user OFDM-CSK after the second layer of security is given by

$$\begin{aligned} e(t) &= x_c(t)\cos(2\pi f_1 t + \varphi_1) + x_u(t)\cos(2\pi f_2 t + \varphi_2) \\ &\quad + \sum_{i=1}^{U} e_i x_u(t) cos(2\pi f_{i+2} t + \varphi_{i+2}), \end{aligned} \tag{4.3}$$

where φ_i represents the phase angle introduced in the carrier modulation process of the ith subcarrier (with frequency f_i). In this chapter the transmitted energy in every subcarrier is normalised.

4.2.2 Receiver

The OFDM-CSK receiver is illustrated as a block diagram in Figure 4.4. A set of correlators is considered, each demodulating the desired signal of the corresponding carrier frequency f_i. The signals are then sampled every kT_c seconds. Assuming that perfect symbol and carrier synchronisation of the OFDM is realised at the receiver, it is assumed that our channel exhibits additive white Gaussian noise (AWGN). In addition, it is assumed that there is no interference between subcarriers. In this case, the received signal is evaluated for one user [15, 16]. After removing artificial noise and cyclic extension, the received signal can be written as

$$r(t) = e(t) + n(t), \tag{4.4}$$

where $n(t)$ is AWGN noise with zero mean and power spectral density of $N_0/2$ plus interference from other secondary users. After applying a fast Fourier transform (FFT) on the received signal, the output at the ith subcarrier (removing the time

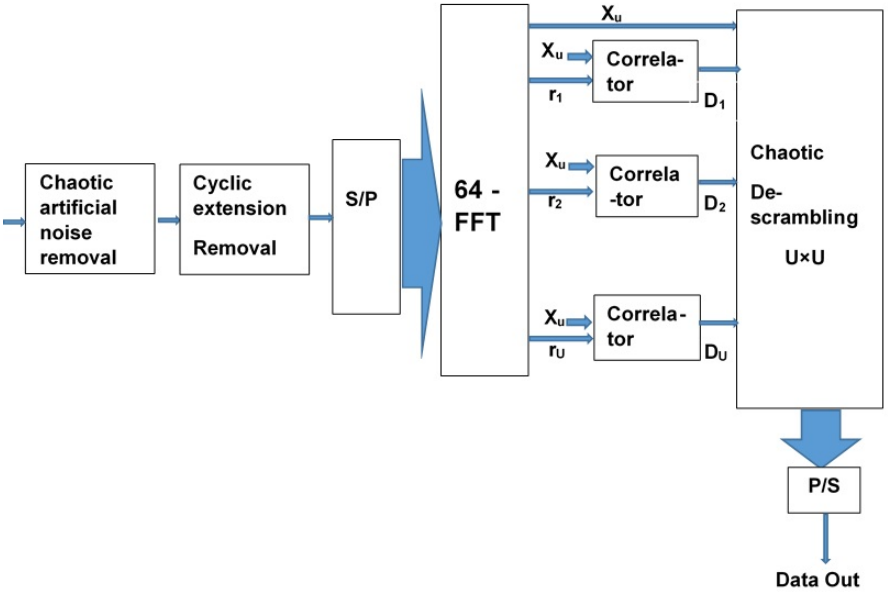

Figure 4.4: Block diagram of the OFDM-CSK receiver

index, t, for notational convenience) is given by

$$r_i = y_i + n_i, \tag{4.5}$$

where $y_i = e_i x_u$ and n_i is the additive white Gaussian noise. The output of each matched filter is given by

$$d_i = \sum_{k=1}^{\beta} r_i x_{u,k} = s_1 \sum_{k=1}^{\beta} x_{u,k}^2 + v_i, \tag{4.6}$$

where $i = 1, 2, 3, \ldots, U$ and $x_{u,k}$ is the kth sample of x_u. Here, it holds that

$$v_i = \sum_{k=1}^{\beta} [x_u v_{k,i} + e_{-i} x_{-u} x_u], \tag{4.7}$$

where $e_{-i}x_{-u}$ represents interference from other secondary users. An equal gain is used, combining as an equaliser on the receiver side with equalisation coefficients as follows:

$$E_\varphi = \frac{(H_\varphi)^\star}{|H_\varphi|}, \tag{4.8}$$

where H_φ is the transfer function of the channel, $(\star)$ represents the conjugation relation and $|H_\varphi|$ is the amplitude of transfer function. This equalisation method

corrects for the phase shift due to the channel. The information bit a_i of the ith correlation detector can be recovered after equalisation as

$$a_i = \text{sign}(d_i). \tag{4.9}$$

A descrambling process is then applied with the same initial condition as for the transmitter to a_i to detect the transmitted bits.

4.2.3 Design of chaotic scrambling and CSK modulation

Enhancing the physical layer security is an important goal of our proposed system. As shown later in Equation (4.17), the chaotic map parameter and initial condition of the chaotic sequence have a considerable impact on the overall BER. Therefore, two layers of encryption are proposed by combining chaotic modulation and scrambling to improve the diffusion property of the encrypted data. The scrambling matrix represents the first layer of encryption and is generated by the following algorithm. A new position matrix $\mathbf{P}$ of the same size $U \times U$ as in (1) is generated, wherein the position elements signify the location of 1 in the scrambling matrix $\mathbf{S}$. The design methodology of the position matrix is based upon the mixing property of chaotic dynamical systems. The mixing property is defined in the following way [17]: For any two open intervals I and J (which can be arbitrarily small, but must have a nonzero length), one can find initial values in I which, when iterated, will eventually lead to points in J. Each sub-domain chaotic map is sequentially numbered from 0 to $U-1$. In the scrambling matrix design, each row has one '1', the remaining elements are zero, and no two rows are the same. For each scrambling matrix, a new key is used, with each key specifying a mapping to a unique combination. The matrix, when multiplied with constellation symbols, scrambles the position of the elements. It is difficult to recover the data with a different key. Due to the characteristics of CR, such as a wireless LAN, attackers can store and read all the traffic of the CR. Consequently, chaotic scrambling is useful to provide each encrypted frame with a specific initial condition. Let the scrambled version of the first frame $\mathbf{e}_1$

with length U be denoted by $\mathbf{c}_1 = CS(\mathbf{e}_1, x_c(C_1))$, where CS denotes the chaotic scrambling process described above, $x_c(\cdot)$ is the logistic chaotic function, and C_1 is initial condition of the chaotic map for the first frame. In general, for the nth frame, it holds that

$$\mathbf{c}_n = CS(\mathbf{e}_n, x_c(C_n)), \tag{4.10}$$

in which $x_c(C_n)$ can be written as

$$x_c(C_n) = \psi \times x_c(C_{n-1})(1 - x_c(C_{n-1})), \tag{4.11}$$

where $3.75 \leq \psi \leq 4$, and $x_c(C_n)$ is the current state of the chaotic map while $x_c(C_{n-1})$ is its previous state. Note that $x_c(C_n)$ has a value between [0, 1].

The second layer of encryption is represented by CSK modulation, which provides random sequences of samples that modulate and spread each frame of the output scrambled data, $\mathbf{c}_n$, with a specific initial condition according to the formula

$$\mathbf{u}_n = CSK(\mathbf{c}_n, x_u(C_n)), \tag{4.12}$$

where CSK is the chaotic shift keying modulating function, and $x_u(\cdot)$ is the third-order Chebyshev map function, as this map satisfies the necessary conditions of the optimum BER, which is shown later in the next section. In our proposed system, the characteristic of the third-order Chebyshev map is written as

$$x_u(C_n) \;=\; c_1 x_u^3(C_{n-1}) - c_2 x_u(C_{n-1}), \tag{4.13}$$

or

$$g_n(\cos\phi) \;=\; c_1 g_{n-1}^3(\cos\phi) - c_2 g_{n-1}(\cos\phi), \tag{4.14}$$

where the current state of chaotic signal, $x_u(C_n) = g_n(\cos\phi)$, depends upon the previous state, $x_u(C_{n-1})$, of the chaotic map. Note that $x_u(C_{n-1}) = g_{n-1}(\cos\phi)$ and $c_1 = 4$ and $c_2 = 3$ are the chosen chaotic map parameters in this work, while $x_u(\cdot)$ has values between [-1, 1]. The characteristic of the third-order Chebyshev map of chaos is shown in Figure 5.14. The malicious eavesdropper must have the same initial condition and chaotic map parameters to be able to decrypt the data.

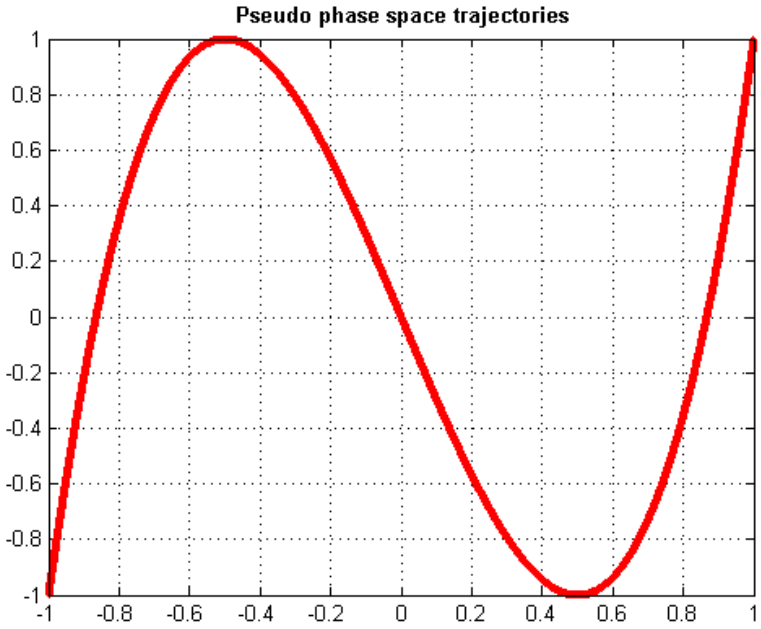

Figure 4.5: Characteristic of the third-order Chebyshev map

4.3 Analysis of BER performance

In this section, analytical expressions are derived for the bit error rate (BER) of an OFDM-based CSK scheme. Here the analysis for the discrete-time case is presented. By applying a Gaussian approximation and the central limit theorem, approximate analytical expressions are obtained for the BER for sufficiently large spreading factors. It can be seen that all sum items in Equation (4.6) can be regarded as zero-mean Gaussian random variables. Hence, the decision parameter y_i in Equation (4.6) can be obtained as

$$y_i = d_i \sum_{k=1}^{\beta} x_{u,i}^2 + \sum_{j=1, j\neq i}^{N} d_j \sum_{k=1}^{\beta} x_{u,i} x_{u,j} + \sum_{k=1}^{\beta} x_{u,i} v_i, \tag{4.15}$$

where N is the number of secondary users, and d_j and $x_{u,j}$ are the transmitted data and spreading sequence of other secondary users, respectively. From an independence feature between chaotic sequences, both $cov[x_{u,i}^2, x_{u,j}^2]$ and $E[x_{u,i}, x_{u,j}]$ must be equal to zero. Under this assumption, the variance of y_i can be formulated

as

$$var\left[y_i\right] = \beta(var\left[x_{u,i}^2\right] + E[x_{u,i}^2] \sum_{j=1,j\neq i}^{N} E[x_{u,j}^2] + E[x_{u,i}^2]N_0/2), \tag{4.16}$$

where $E\left[.\right]$ represents the expectation operator, $N_0/2$ is the power spectral density of Gaussian noise, and $var\left[.\right]$ denotes the variance operator. Each correlation detection output, U_i, can be regarded as an independent Gaussian variable for large β. Thus, the overall optimum BER can be achieved as in [19]:

$$BER = \frac{1}{2}\text{erfc}\left[\left(\frac{2\nu}{\beta} + \frac{2(N-1)}{\beta} + \left(\frac{E_b}{N_o}\right)^{-1}\right)^{-1/2}\right], \tag{4.17}$$

where E_b/N_0 is the SNR per bit, $\nu = var[x_{u,i}^2]/P_s^2$, $P_s = E[x_{u,i}^2]$, and ν must be same for all users. However, the above BER is achieved only if the chaotic map satisfies the following conditions [18]:

c1) Different users have chaotic sequences with very low cross-correlations even for a finite length; that is, $cov[x_k^2, x_m^2] = 0$, where x_k and x_m are different chaotic sequences.

c2) The bit energy is kept constant for each user.

c3) $E[x_k, x_m] = 0$.

In the following, it will be shown that the chaos-based Chebychev map satisfies these three conditions. In general, for the Chebyshev map of degree N, it is the case that

$$g_N^k(\cos\varphi) = \cos(N^k\varphi). \tag{4.18}$$

Moreover, the invariant probability density function (pdf) of $\cos\varphi$ can be shown to be

$$\sigma(x) = \begin{cases} \frac{1}{\pi sin\varphi} & \text{if } 0 \leq x \leq \pi \\ 0 & \text{otherwise.} \end{cases} \tag{4.19}$$

- *Proof of condition (c1) and (c2)*: It holds that

$$cov\left[x_k^2, x_m^2\right] = E[x_k^2, x_m^2] - E\left[x_k^2\right] E\left[x_m^2\right]. \tag{4.20}$$

Considering the case where $k \neq m$. Without a loss of generality, it can be assumed that $k = n + m$ for some positive integer. Then

$$\begin{aligned} E[x_k^2, x_m^2] &= \int_{-\infty}^{\infty} x^2 \left(g_m^n(x)\right)^2 \rho(x) dx \\ &= \int_{-1}^{1} x^2 \left(g_m^n(x)\right)^2 \frac{1}{\sqrt{1-x^2}} dx. \end{aligned} \tag{4.21}$$

Using (4.18) and $x = \cos\varphi$, Equation (4.21) can be written as

$$E[x_k^2, x_m^2] = \frac{1}{\pi} \int_0^{\pi} cos^2(\varphi) \left(g_m^n(cos\varphi)\right)^2 d\varphi = \frac{1}{4}. \tag{4.22}$$

Furthermore, $E\left[x_k^2\right]$ can be derived as

$$E\left[x_k^2\right] = \int_{-\infty}^{\infty} x^2 \rho(x) dx = \int_{-1}^{1} x^2 \frac{1}{\pi\sqrt{1-x^2}} dx = \frac{1}{2}. \tag{4.23}$$

Combining Equation (4.20), (4.22), and (4.23) yields $cov\left[x_k^2, x_m^2\right] = 0$.

- *Proof of condition (c3)*: With $k \neq m$ and some positive integer n, and replacing $x = \cos\varphi$, the cross-correlation, $E\left[x_k x_m\right]$, is achieved as

$$\begin{aligned} E\left[x_k x_m\right] &= \int_{-\infty}^{\infty} x \left(g_m^n(x)\right) \rho(x) dx \\ &= \frac{1}{\pi} \int_0^{\pi} \cos\varphi \left(g_m^n(\cos\varphi)\right) d\varphi = 0. \end{aligned}$$

4.4 Enhancing secrecy using chaotic artificial noise

In this section, the objective is to improve the secondary secrecy rate via transmitting appropriate jamming signals, as the eavesdropper may intercept the reference chaotic signals at frequencies f_1 and f_2. There is no extra jammer, but *a-priori* knowledge of jamming signals is available at legitimate receivers.

To enhance secrecy, the legitimate transmitters are allowed to use some of their power to transmit a jamming signal, in addition to transmitting the message signal. According to the secrecy capacity of wiretap channels addressed in [25], it has been shown that for input s, the secrecy capacity, C_{sec}, is given by

$$\begin{aligned} C_{sec} &= \max_{s}[I(s,x) - I(s,x_E)] \geq \\ &\quad \max_{s}[I(s,x)] - \max_{s}[I(s,x_E)], \end{aligned} \tag{4.24}$$

where x and x_E are the received signals in legitimate and eavesdropper receivers, respectively. Here it is considered that any pair of mutual information $(I(s,x), I(s,x_E))$ for messages x and x_E is said to be achievable if the average error probabilities $P_{e,1} = \Pr(\hat{x} \neq x)$ and $P_{e,2} = \Pr(\hat{x}_E \neq x_E)$ can be made arbitrary small. The secrecy rate can be defined as

$$\begin{aligned} R_{sec} &= \max_{s}[I(s,x)] - \max_{s}[I(s,x_E)] \\ &= \max(R_D - R_E)^+, \end{aligned} \tag{4.25}$$

where R_D is the information rate at the destination and R_E is the leakage rate at the eavesdropper; and $(x)^+ = \max(0,x)$ refers to the positivity value of the secrecy rate. For convenience, the $(\cdot)^+$ sign from is removed from subsequent calculations. The received signal at the secondary receiver, x_R, can be written as

$$x_R = \sqrt{\epsilon P_s} h_{ss} u + \sqrt{(1-\epsilon)P_s} h_{ss} z + n_R + n_I, \tag{4.26}$$

where u is the transmitted signal at the output of Layer 3; P_s is the transmission power; ϵ is the power fraction used to transmit data ($0 < \epsilon < 1$); $h_{ss} \sim \mathcal{CN}(0, \sigma_h^2)$ comprises the channel coefficients between the secondary transmitter and receiver; $n_R \sim \mathcal{CN}(0, \sigma^2)$ is the AWGN at the secondary receiver and n_I an interference from other secondary users; and z is an artificial noise generated by a linear feedback shift register (FSR), which is controlled by chaotic signal-based Chebyshev map according to the following equations [30]:

$$x_u(C_n) = c_1 x_u^3(C_{n-1}) - c_2 x_u(C_{n-1}) \tag{4.27}$$

$$z = Q(x_u(C_n)), \tag{4.28}$$

where $Q(\cdot)$ is a 3-bit quantiser function. According to conditions $(c1)$ and $(c3)$ in Section III, and using a Chebyshev map as the chaotic sequence in Layers 2 and 3 of the C-OFDM transmitter, n_I can be neglected due to zero cross-correlation between secondary users. For notational convenience, let us define

$$\rho_{ss} = \frac{P_s {h_{ss}}^2}{\sigma^2}.$$

It is assumed that the ST is aware of artificial noise. The rate at the secondary transmitter, R_{ss}, is written as

$$R_{ss} = \frac{1}{2}\log(1 + \epsilon\rho_{ss}). \tag{4.29}$$

Furthermore, the received signal at the eavesdropper can be written as

$$x_E = \sqrt{\epsilon P_s}h_{se}u + \sqrt{(1-\epsilon)P_s}h_{se}z + n_E, \tag{4.30}$$

where $n_E \sim \mathcal{CN}(0, \sigma^2)$ and $h_{se} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel between the secondary transmitter and eavesdropper. The rate at the eavesdropper is then

$$R_{se} = \frac{1}{2}\log_2(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}), \tag{4.31}$$

where

$$\rho_{ss} = \frac{P_s {h_{se}}^2}{\sigma^2}.$$

According to Eq. (4.25), the achievable secrecy rate, R_{sec}, can be calculated as

$$R_{sec} = R_{ss} - R_{se} \tag{4.32}$$

$$R_{sec} = \log_2(1 + \epsilon\rho_{ss}) - \log_2(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}). \tag{4.33}$$

4.4.1 Optimisation of the secrecy rate

The secondary transmitter can optimise ϵ to maximise the secrecy rate. First, the following property holds:

Lemma 1. *The secrecy rate of secondary transmission in Eq.* (4.33) *is concave in terms of* ϵ.

Proof: See Appendix A ■

As the secrecy rate is concave in terms of ϵ, it is possible to find the optimum value of ϵ^* to maximise the secrecy rate. ϵ^* can be found from the following equations:

$$\frac{\partial R_{sec}}{\partial \epsilon} = \left(\frac{\rho_{ss}}{(1+\epsilon^* \rho_{ss})} - \frac{\rho_{se}}{(1+(1-\epsilon^*)\rho_{se})} \right) \tag{4.34}$$

$$\epsilon^* = \frac{\rho_{ss} - \rho_{se} + \rho_{ss}\rho_{se}}{2\rho_{ss}\rho_{se}}. \tag{4.35}$$

Therefore, the optimum solution that maximises R_{sec} is given by

$$\epsilon^* = \arg\max R_{sec}(\epsilon). \tag{4.36}$$

4.5 Extension to multiple eavesdroppers

In this case, all the eavesdroppers are distributed on a two-dimensional plane according to a homogeneous (PPP) distribution ϕ_e with density λ_e around N ST-SR pairs. This means that eavesdroppers are distributed randomly with different distances around legitimate STs, as shown in Figure 5.12. As a worst-security case, it is assumed that each eavesdropper is similar to a legal receiver, which can cancel the interference caused by other $(N-1)$ STs due to low cross-correlation between secondary users. This assumption is useful to highlight the effect of interference caused by the chaotic artificial noise. Furthermore, equal transmission power is assumed amongst the STs (i.e., $P_{s,k} = P_s/N$) and $E[|h_{se}|^2] = 1$. In this scenario, two important performance metrics are considered: secrecy outage probability and mean secrecy rate.

4.5.1 Secrecy outage probability of multiple eavesdroppers

The signal-to-interference-and-noise ratio (SINR) of any particular eavesdropper (with distance $d_{e,k}$ to the considered kth ST) is given by

$$\gamma_{e,k} = \frac{\epsilon P_{s,k} |h_{se}|^2}{\sigma^2 d_{e,k}^{\alpha} + (1-\epsilon) P_{s,k} |h_{se}|^2}$$

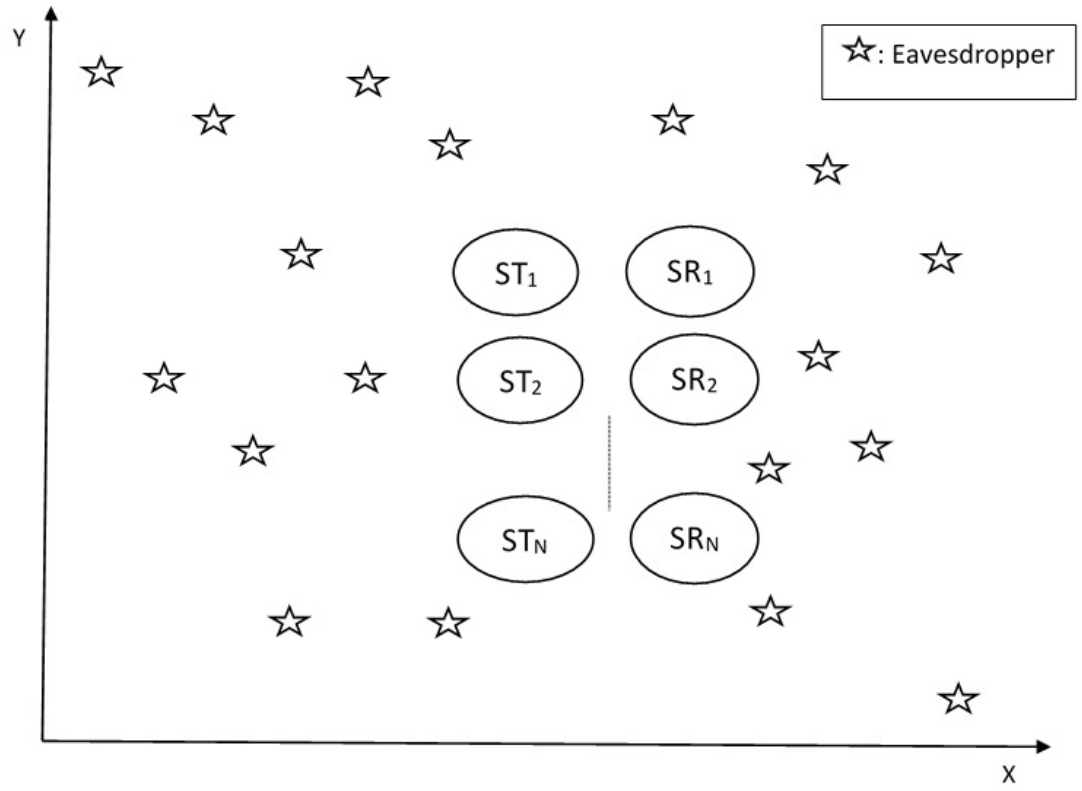

Figure 4.6: Distribution of eavesdroppers around ST-SR pairs

$$= \frac{\epsilon P_s \left|h_{se}\right|^2}{\sigma^2 d_{e,k}^{\alpha} N + (1-\epsilon) P_s \left|h_{se}\right|^2}. \tag{4.37}$$

The outage probability is defined as the probability that any eavesdropper has an SINR greater than or equal to the SINR of the legitimate destination, denoted by γ_k where $k = 1, 2, ..., N$. The special case of the most malicious eavesdropper to the kth ST, $\gamma_{E,k}$, becomes

$$\gamma_{E,k} = \max_{e \in \phi_e} \frac{\epsilon P_s \left|h_{se}\right|^2}{\sigma^2 d_{e,k}^{\alpha} N + (1-\epsilon) P_s \left|h_{se}\right|^2}. \tag{4.38}$$

Lemma 2. *The secrecy outage probability between the kth SR and the most malicious eavesdropper is written as*

$$P_{o,k} = 1 - \exp\left[\frac{2\pi\lambda_e}{\alpha}\left(\frac{(\epsilon - (1-\epsilon)\gamma_k)P_s}{N\gamma_k\sigma^2}\right)^{\frac{2}{\alpha}}\Gamma\left(\frac{2}{\alpha}\right)\right], \tag{4.39}$$

where $\Gamma(.)$ *is the Gamma function, and is given by*

$$\Gamma(x) = \int_0^\infty t^{(x-1)} e^{-t} dt.$$

Proof: See Appendix B. ■

The following presents the special case in which the path loss exponent is equal to 4, which is commonly used for practical scenarios of large-scale wireless networks [33, 34].

Lemma 3. *With the path loss exponent equal to 4, the secrecy outage probability between the kth SR and the nearest eavesdropper is given by*

$$P_{o_E,k} = \frac{\pi^{3/2}\lambda_e\sqrt{(\epsilon-(1-\epsilon)\gamma_k)P_s}}{2\sqrt{N\gamma_k\sigma^2}} \exp\left[\frac{\pi^2{\lambda_e}^2}{\frac{4N\gamma_k\sigma^2}{(\epsilon-(1-\epsilon)\gamma_k)P_s}}\right] erfc\left(\frac{\pi\lambda_e}{2\sqrt{\frac{N\gamma_k\sigma^2}{(\epsilon-(1-\epsilon)\gamma_k)P_s}}}\right). \quad (4.40)$$

Proof: See Appendix C. ■

Remark 1. The following observations can be seen from Lemma 2 and Lemma 3:

1. The secrecy outage probability approaches 0 as N goes to infinity.
2. The secrecy outage probability is decreased significantly when the allocated power $P_s(1-\epsilon)$ for artificial noise is increased.
3. The ratio between the allocated power for the signal and artificial noise is limited by $\frac{\epsilon}{(1-\epsilon)} \geq \gamma_k$ according to Equations (4.39) and (4.40).
4. The secrecy outage probability increases with increasing λ_e.

4.5.2 Mean secrecy rate

In this subsection, the mean secrecy rate, averaged over the random locations of the eavesdroppers, is derived. The following result is obtained for the mean secrecy rate at the kth SR when the interference between multiple ST-SR pairs is neglected according to conditions (c1) and (c3) in Section III.

Lemma 4. *The mean secrecy rate achievable at the kth SR by employing C-OFDM and artificial noise in CR systems is*

$$\begin{aligned}\mathbb{E}_{\phi_e}[R_k|\gamma_k > \gamma_{e,k}] &= \log_2(1+\gamma_k)^{1-P_{o_E,k}} \\ &\quad - \int_{\gamma_{min}}^{\gamma_k} f_{\gamma_{e_0,k}}(x)\log_2(1+x)dx,\end{aligned}$$

where $\gamma_{E,k}$ and γ_{min} are the SINR between the kth SR and the nearest eavesdropper and the most distant eavesdropper, respectively. It is then the case that

$$\begin{aligned}f_{\gamma_{E_0,k}}(x) &= -\frac{a\epsilon}{2\sqrt{\pi}x^3\sqrt{\frac{\epsilon}{x}+\epsilon-1}}\left(\sqrt{\pi}e^{b^2\left(\frac{\epsilon}{x}+\epsilon-1\right)}\right. \\ &\quad \left(2b^2(\epsilon x+\epsilon-x)+x\right) erfc\left(b\sqrt{\frac{\epsilon}{x}+\epsilon-1}\right) - \\ &\quad \left. 2bx\sqrt{\frac{\epsilon}{x}+\epsilon-1}\right), \qquad (4.41)\end{aligned}$$

where $a = \frac{\pi^{\frac{3}{2}}\lambda_e}{2}\sqrt{\frac{P_s}{N\sigma^2}}$ and $b = \frac{\pi\lambda_e}{2}\sqrt{\frac{P_s}{N\sigma^2}}$.

Proof: See Appendix D. ■

Remark 2. The following observations arise from Lemma 4:

1. The mean secrecy rate increases significantly as N goes to infinity due to the secrecy outage probability approaching 0.

2. The mean secrecy rate increases significantly as ϵ approaches 0 due to the decreasing secrecy outage probability.

4.6 Simulation results and discussion

In the CR-based chaotic OFDM-CSK system, a Chebyshev map is used to generate a chaotic sequence. The system is applied in spectrum overlay, or opportunistic

spectrum access (OSA), wherein secondary users aim to exploit frequency bands that are not used by primary users in a particular geographical area. In this scheme, there are no power limits placed on secondary users because of the absence of interference with primary users.

In a simulation, the following parameters are considered: 2 secondary users, 2 primary users, data rate = 10kbps, symbol period $T_b = 100\mu$sec, spreading factor β = 12/25/50, FFT length = 64, data subcarriers = 52, and a Rayleigh fading channel with AWGN. The number of taps for the Rayleigh fading channel, in the comparison between traditional and chaotic OFDM, is 10 in overlay spectrum access.

Figure 4.7 shows the BER performance of CR-based MC-CSK for different lengths of spreading codes in the overlay scenario. The BER is improved by using a longer spreading code according to Eq. (4.17).

Regarding the scrambling and CSK process, when the same data are recovered with a slightly different initial condition for the chaos generator between transmitter and receiver, nearly all of the constellation symbols are in error. The probability of error is uniformly distributed in symbols. To test the effect of chaotic scrambling/modulation, the proposed chaotic scrambling is applied in OFDM with QPSK. It is assumed that the initial condition value for the chaotic map in the legal receiver is 0.095, while the eavesdropper with the illegal receiver has an initial condition value for the same chaotic map of 0.095000001.

The simulation results for the BER are shown in Figure 4.8. It is confirmed that with the slightly difference of 10^{-9} in the initial conditions between the legal and illegal receivers, the illegal receiver yields a much higher BER by using the proposed chaotic scrambling than by scrambling the sample sequence within each time-domain OFDM symbol. This phenomenon is equivalent to a constellation transformation over each subcarrier in the frequency domain [20]. Therefore, this result confirms that enhancement in a low-data interception feature due to the proposed system encrypts each frame with the specific initial condition of chaotic scrambling. Also, it is difficult for a passive attacker to sniff encrypted frames with different chaotic

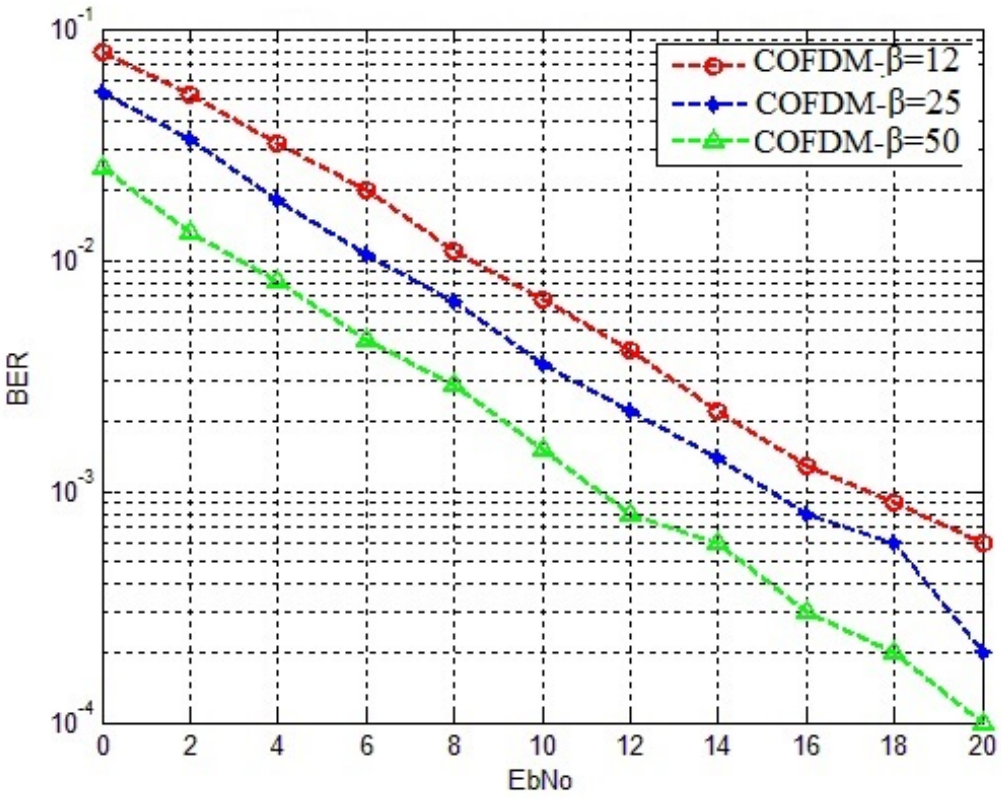

Figure 4.7: BER performance of the proposed system for different lengths of spreading code in CR-based overlay spectrum access

initial conditions.

It is necessary to investigate the effect of a slight error in the parameter of the chaotic map that generates the chaotic signal for CSK on BER performance of the illegal C-OFDM-based receiver (with no error in scrambling process). Figure 4.9 shows that the illegal receiver still has a very high BER compared to that of the legal C-OFDM receiver.

In the above scenarios, the chaotic scrambling and CSK modulation are useful for generating a large key space to resist brute-force attacks and provide a low-interception feature.

The effect of adding chaotic artificial noise to Layer 3 to improve the secrecy rate in two scenarios was investigated as follows:

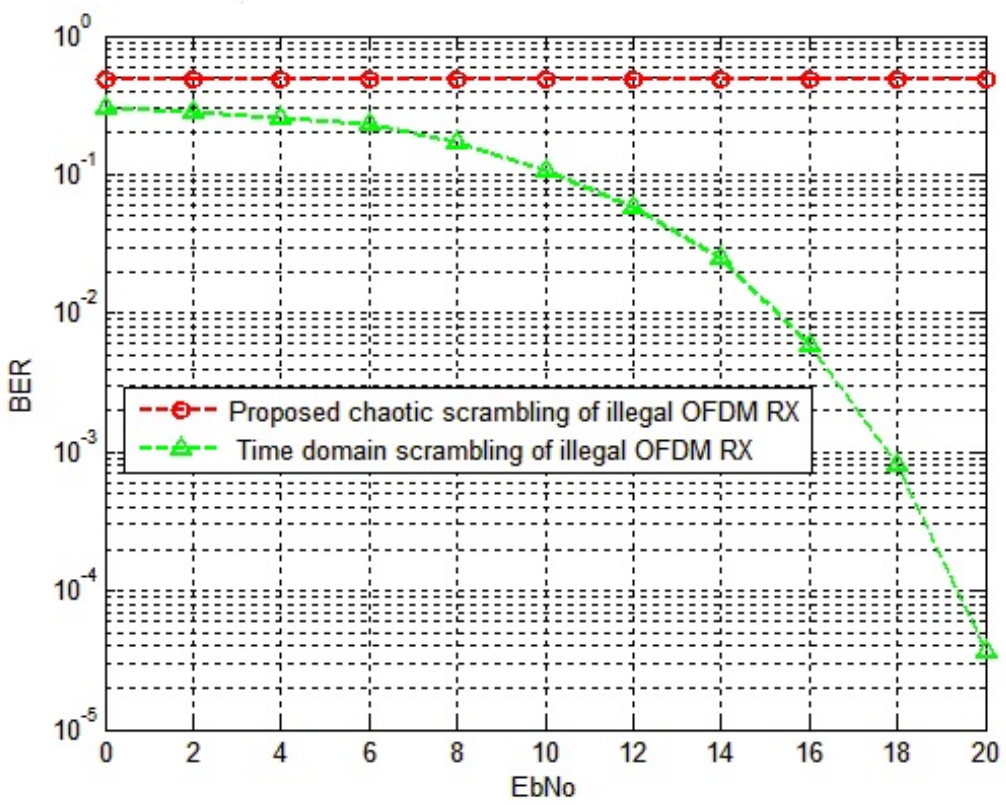

Figure 4.8: Effect of a slight error in the initial condition for chaotic scrambling on the BER of the illegal receiver

i) Scenario I - Single eavesdropper: In this scenario, the location of the legitimate transmitter is fixed at the (0,0) coordinate to determine the effect of eavesdropper position on the secrecy rate. Three schemes are considered depending on the location of the single eavesdropper: Location I (0.6,0), Location II (1.0,0), and Location III (1.2,0). It is assumed that that the path loss model $h = d^{-\alpha}$ is used with path loss exponent $\alpha = 3.0$.

Figure 4.10 represents the effect of distance between the legitimate transmitter and receiver on the secrecy rate with respect to the position of the single eavesdropper. The secrecy rate decreases significantly with increasing distance due to the decrease in ρ_{ss} in Eq. (4.33) between the source and destination. Moreover, the secrecy rate is increased when the eavesdropper is located farther away from the

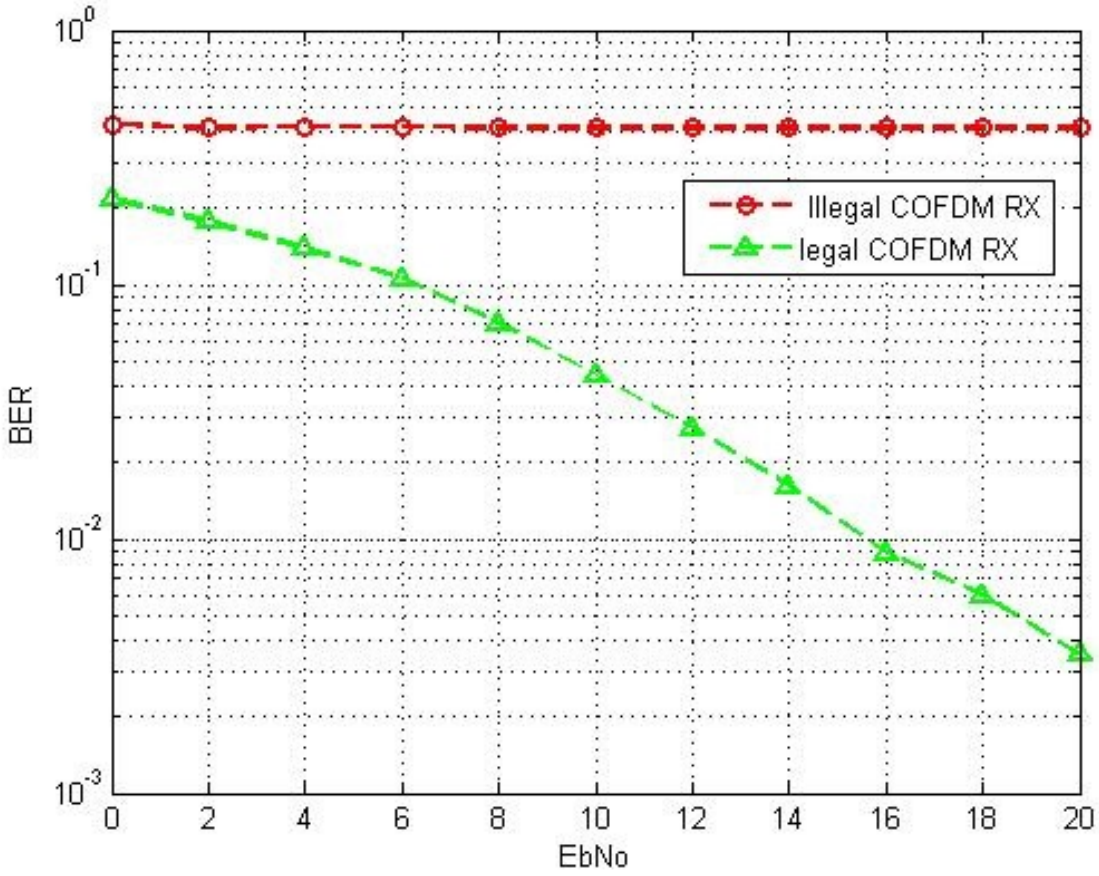

Figure 4.9: Effect of a slight error in the parameters of chaotic modulation on the performance of the illegal receiver

legitimate transmitter due to the decrease in ρ_{se}.

Figure 4.11 shows the effect of SNR on the secrecy rate with respect to position of the single eavesdropper and the location of the legitimate receiver at the coordinates of (0.5,0). It is evident from this figure that the secrecy rate increases significantly with increasing SNR.

Figure 4.12 shows the effect of the allocated power ϵ on the secrecy rate with respect to the position of the single eavesdropper with the legitimate receiver located at the same coordinates of (0.5,0). This indicates that the secrecy rate is a concave function with respect to ϵ, according to Eq. (4.35).

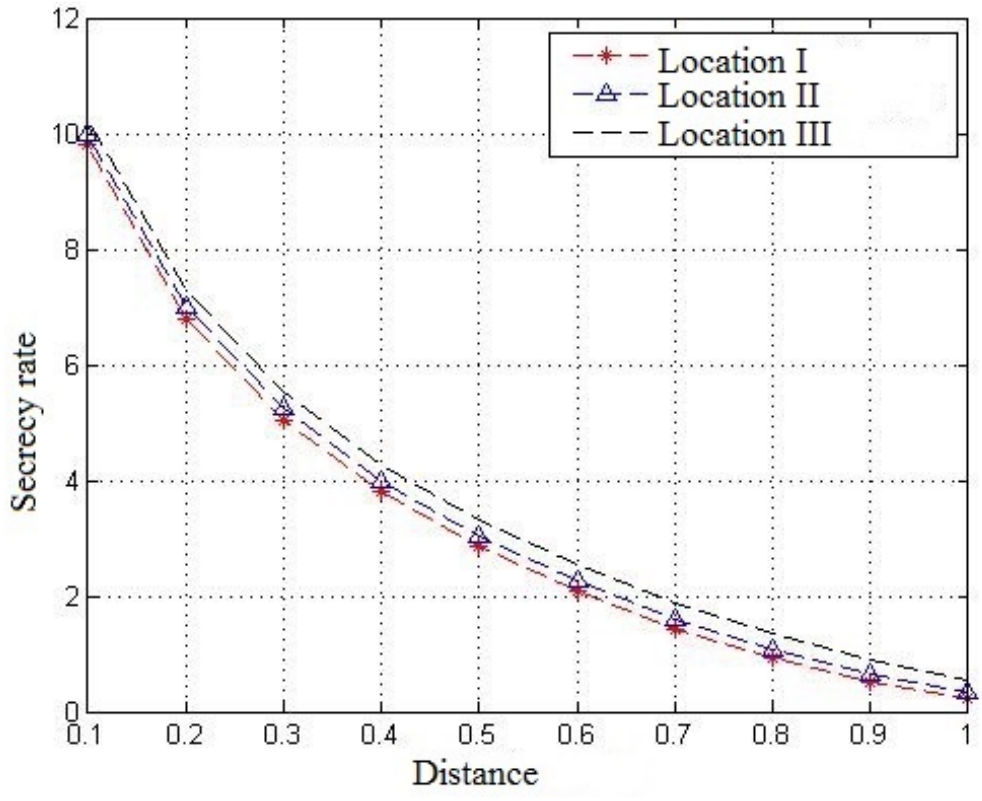

Figure 4.10: Secrecy rate vs. distance between the legitimate transmitter and receiver

Figure 4.13 shows that the optimal allocated power fraction, ϵ^*, decreases with increasing distance between the legitimate transmitter and receiver, according to Eq. (4.36), due to the increased allocated power fraction of artificial noise $(1 - \epsilon^*)$ for maintaining an acceptable secrecy rate when the legitimate transmitter is closer to the eavesdropper than to the legitimate receiver. On the other hand, ϵ^* increases when the eavesdropper is located farther away, due to the decrease of ρ_{se} in Eq. (4.35).

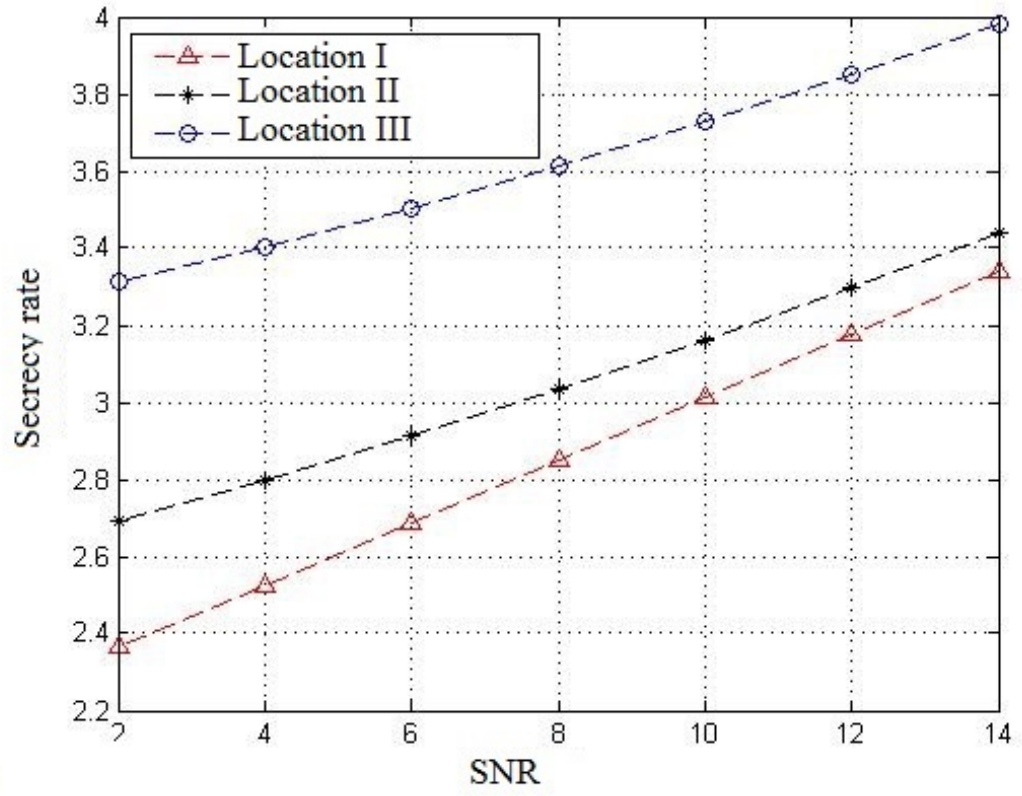

Figure 4.11: Secrecy rate vs. SNR

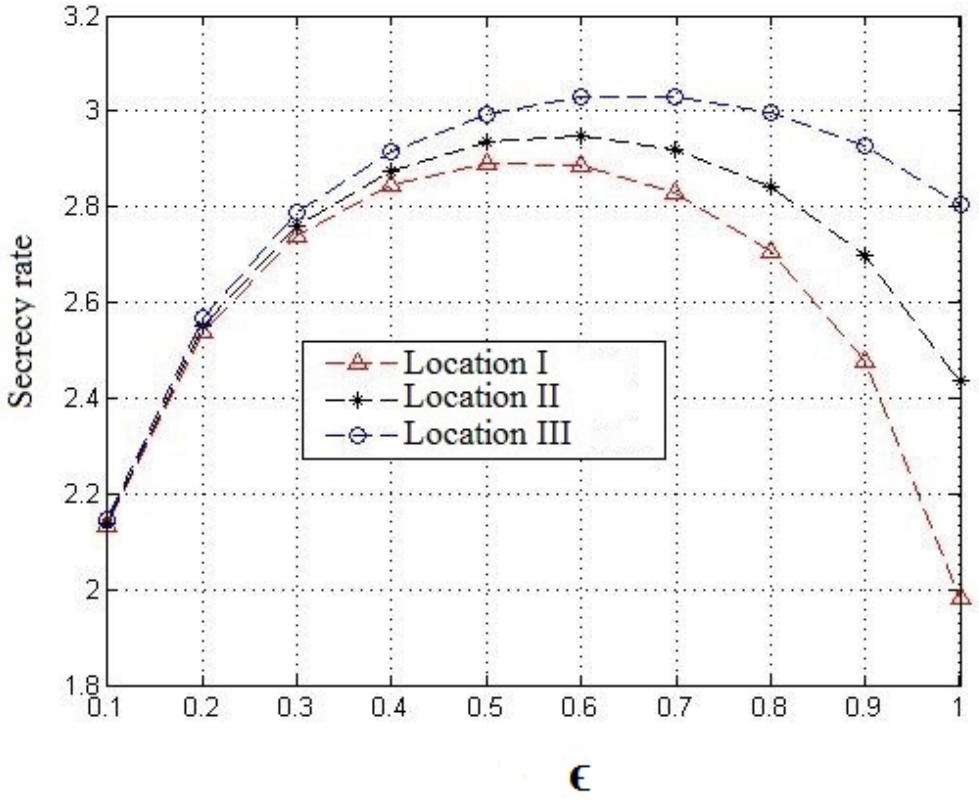

Figure 4.12: Secrecy rate vs. ϵ

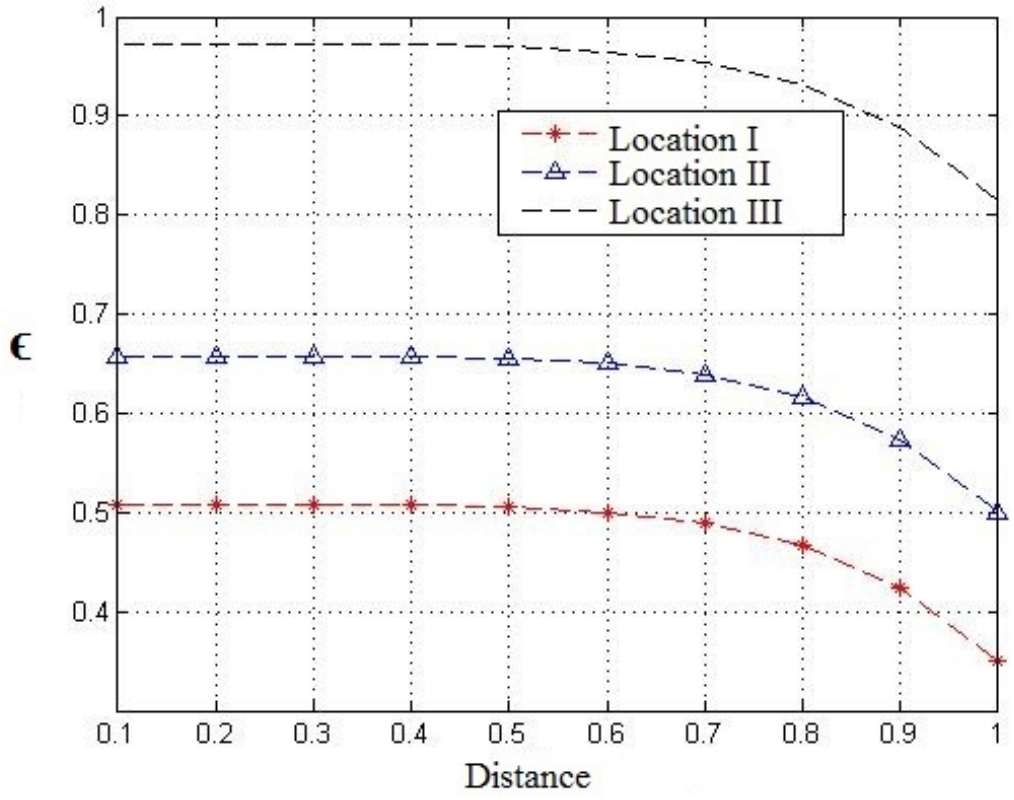

Figure 4.13: Optimal allocated power fraction (ϵ^*) vs. distance between the legitimate transmitter and receiver

ii) Scenario II - Multiple eavesdroppers: This scenario considers the secrecy outage probability and mean secrecy rate of a C-OFDM CR system with multiple eavesdroppers. Here, it is assumed that $\lambda_e = 0.1, \sigma^2 = 10^{-4}$, $\gamma_k = -1dB$, and $\gamma_{min} = -5dB$. Figure 4.14 compares the secrecy outage probability of the proposed system with chaotic artificial noise (of various values of ϵ) and without artificial noise. The secrecy outage probability decreases with an increasing number of ST−SR pairs. Moreover, the secrecy outage probability is reduced significantly by chaotic artificial noise in comparison with no artificial noise, and this is consistent with our finding in Remark 1. Finally, the secrecy outage probability decreases with decreasing ϵ, due to the increased power allocated to the chaotic artificial noise.

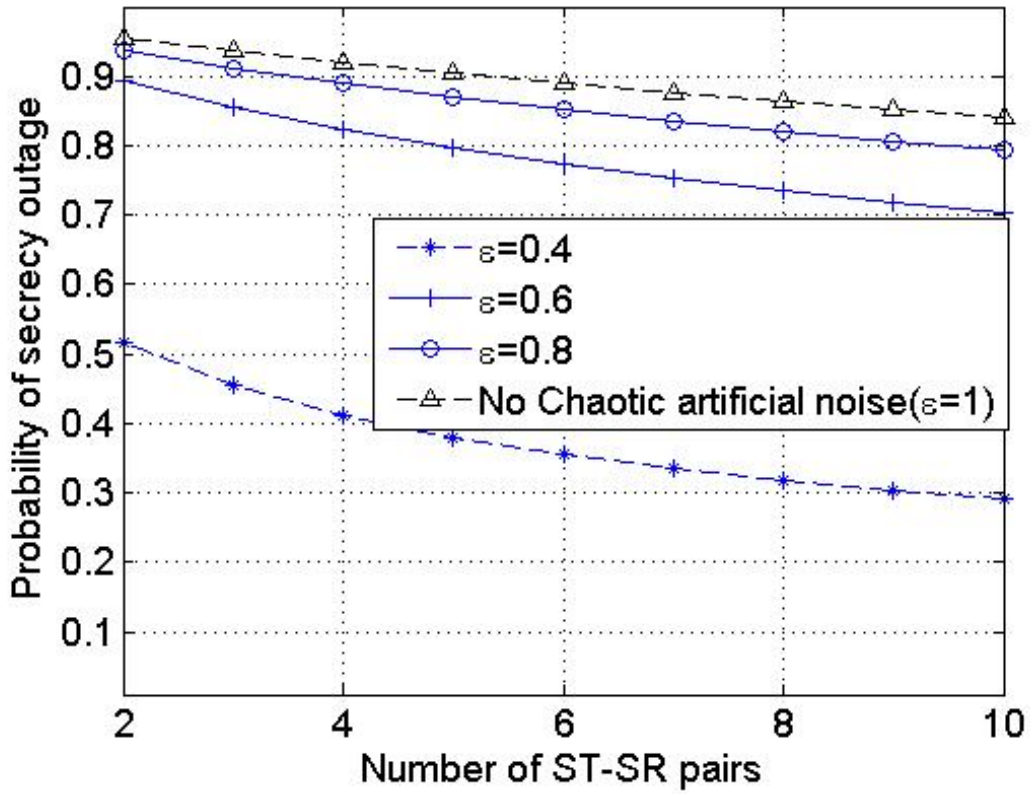

Figure 4.14: Secrecy outage probability vs. number of ST-SR pairs

Figure 4.15 shows that the mean secrecy rate of multiple eavesdroppers increases significantly with the number of ST−SR pairs, whereas it decreases significantly with

increasing ϵ, which is consistent with Remark 2.

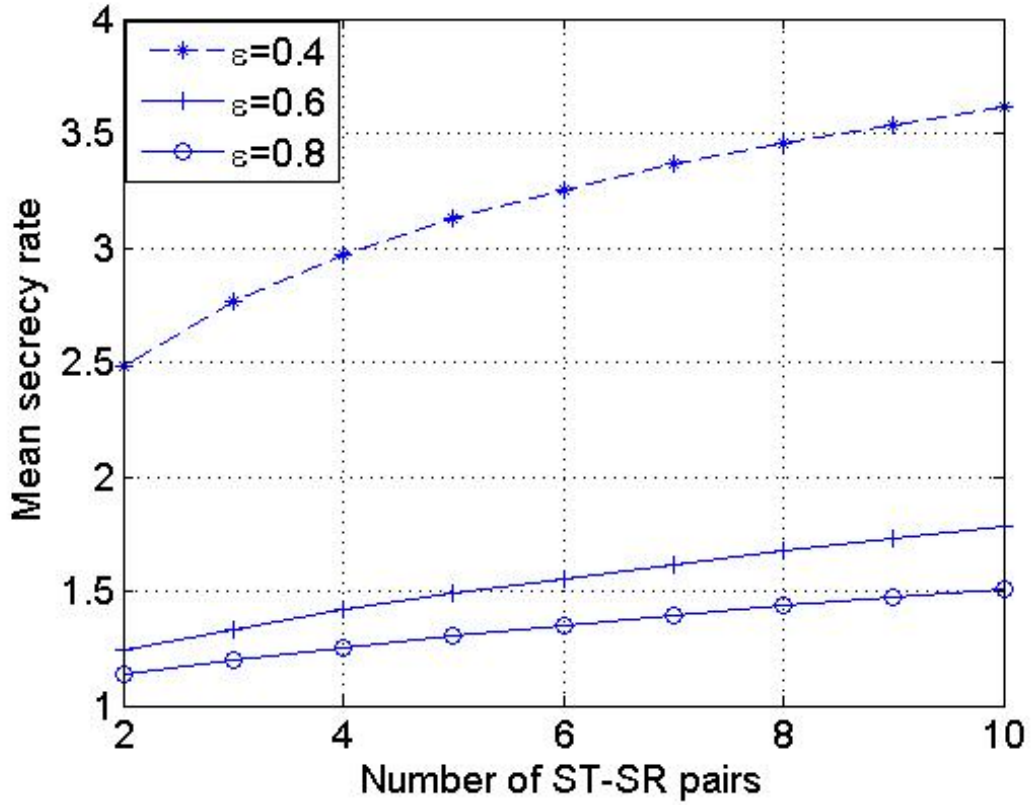

Figure 4.15: Mean secrecy rate vs. number of ST-SR pairs

4.7 Conclusions

This chapter proposed the OFDM-CSK-based CR system with chaotic scrambling and modulation. OFDM-CSK is a non-coherent system that, in contrast to the traditional CSK, does not require reproduction of the chaotic signal at the receiver. A mechanism was proposed to provide three layers of security. In the first layer, the constellation symbols are dynamically scrambled using a scrambling matrix that is generated based on the chaos logistic map. In the second layer, the Chebyshev map-based CSK allows for spreading of each frame of the scrambled data with a specific initial condition and mapping parameters. In the third layer,

chaotic artificial noise was applied to enhance the secrecy rate against malicious eavesdroppers. Our simulation results have shown that two security layers provide a low-interception property and make it difficult for passive attackers to process frames with different initial conditions or different values of the chaotic map parameters. This feature provides a large key space for chaotic scrambling and chaotic modulation to resist malicious attacks. Moreover, both the secrecy rate and secrecy outage probability are improved significantly by C-OFDM for single and multiple eavesdroppers.

Chapter 5

Enhancing physical layer security via Stackelberg game theory

In this chapter, a game theory-based cooperation scheme is investigated to enhance physical layer (PHY) security in both the primary and secondary transmissions of a cognitive radio network (CRN). In CRNs, the primary network may decide to lease its own spectrum for a fraction of time to the secondary nodes in exchange for appropriate remuneration. The secondary transmitter (ST) is considered as a trusted relay for primary transmission in the presence of the eavesdropper (ED) . The ST forwards a message from the primary transmitter (PT) in a decode-and-forward (DF) fashion and, at the same time, allows part of its available power to be used to transmit an artificial noise (i.e., jamming signal) to enhance secrecy rates. Power is allocated between the message and jamming signals via formulation and solution of the optimisation problem for maximising the primary secrecy rate (PSR) and secondary secrecy rate (SSR) with malicious attempts from a single eavesdropper or multiple eavesdroppers. The cooperation between the primary and secondary transmitters is then analysed from a game-theoretic perspective, and model their interaction as a Stackelberg game. The Stackelberg equilibrium is proven theoretically and computed. Finally, numerical examples illustrate the impact of the Stackelberg game-based optimisation on the achievable PSR and SSR. It will be

shown that spectrum leasing, based on trading secondary access for cooperation by means of relay and a jammer, is a promising framework for enhancing primary and secondary secrecy rates in cognitive radio networks when the ED can intercept both the primary and secondary transmission.

5.1 Part I: physical layer security via a Stackelberg game

Inspired by [117], a novel scenario is proposed wherein the ED can intercept the primary and secondary transmissions, and the ST acts as a trusted relay and jammer by allocating part of its transmitted power to emit an artificial noise, creating interference to EDs and thereby protecting the primary and secondary transmissions. The main benefit of this novel scenario is its protection of both the primary and secondary transmissions against eavesdroppers, in contrast to previous studies, which protected only primary transmissions. It is assumed that the primary receiver (PR) and SR have knowledge of artificial noise, in order to overcome the artificial noise at a legal receiver. Two scenarios are studied in which a Stackelberg game theory-based cooperative scheme is used to improve the achievable primary secrecy rate (PSR) and secondary secrecy rate (SSR). In Scenario I, a single ED is considered as shown in Figure 6.1. Here, the PT broadcasts its encoded signal to the ST in Phase 1 under the assumption that the ED is out of range of the PT; then, the ST forwards the primary message with artificial noise to the PR in Phase 2; and finally the ST sends its own signal with artificial noise to the SR in Phase 3. In Scenario II, as indicated in Figure 6.2, the work is extended to multiple eavesdroppers which are located in the range of the ST. The SR is also able to function as a multi-antenna jammer in Phase 1 to reduce the leakage rate at the eavesdroppers. Furthermore, in Scenario II, the following two cases of multiple eavesdroppers are considered in deriving the closed forms of the secrecy rates for ST-PR and ST-SR transmissions:

- *Colluding eavesdroppers*: All eavesdroppers can be seen as a single eavesdropper due to their joint processing action, and the optimal receiver strategy is based on maximum ratio combining, which combines the effects of all eavesdroppers in deriving closed forms for the PSR and SSR [106].

- *Non-colluding eavesdroppers*: The secrecy rate is determined by that of the most malicious eavesdropper, considering that each eavesdropper overhears the primary or secondary communication individually.

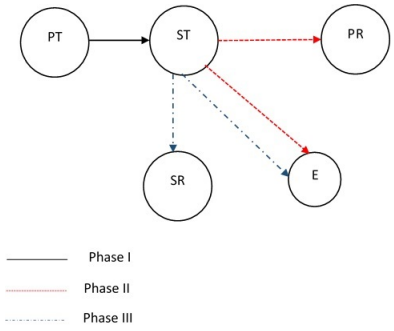

Figure 5.1: Illustration of the cognitive radio (CR) system model in Scenario I

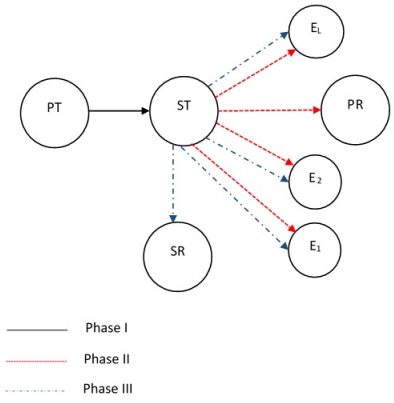

Figure 5.2: Illustration of the CR system model in Scenario II

In such networks, a primary node may lease portions of a licensed spectrum to a secondary node in exchange for some form of compensation. Moreover, retribution from secondary to primary nodes takes the form of cooperative relaying and jamming

to enhance the secrecy of the primary transmission. This scenario avoids the regulatory issues or money transactions that commonly hinder implementation of the property-rights spectrum leasing concept [124].

In the context of the aforementioned schemes, novel system designs—power allocation and time allocation—are proposed for primary and secondary transmissions that maximise the achievable PSR and SSR subject to a total transmit power constraint. Codeword design for meeting the achievable secrecy rates is not considered in this work. The main contributions of this work can be summarised as follows:

- In Scenario I, with a single eavesdropper, an efficient optimisation is provided that maximises both the PSR and SSR under the flat fading channel model. In particular, the primary and secondary power allocation problems at the ST are analysed and solved using time slot allocation of the spectrum lease.

- In Scenario I, the secrecy rates achieved with our proposed 3-phase system are higher than those in other studies ([98],[99]), which are based on an external jammer in the same geometric environment.

- Scenario II studies the design and analysis for the proposed CRNs under malicious attempts by multiple eavesdroppers (colluding and non-colluding eavesdroppers) around the ST to highlight the impact of multiple eavesdroppers on the PSR and SSR. The power allocation problem and time allocation problem are analysed and solved.

- In Scenario II, it is shown that the secrecy rate achieved for CRNs under the colluding eavesdropper is significantly lower than that under non-colluding eavesdroppers.

The remainder of this chapter is organised as follows. In Section II, the system model and achievable secrecy rates are defined in cognitive Scenario I. Section III presents the possible optimisation problems for the given scenarios and their

game-theoretic approach in Scenario II. Those scenarios are then compared through numerical simulations in Section IV. Finally, Section V concludes this chapter.

5.2 Enhancing secrecy rates using a Stackelberg game: a single eavesdropper (Scenario I)

This section considers a cooperative CRN where the ST is allowed to access the primary spectrum, provided that it acts as the jammer for the ED and the relay for the primary transmission as illustrated in Figure 6.1, consisting of the following single antenna nodes: a PT, a PR, a cognitive ST, an SR, and a single ED (i.e., Scenario I). It is assumed that the legal primary destination has *a priori* knowledge of the jamming signal sent by the ST (relay), and the secondary destination has *a priori* knowledge of the jamming signals sent by the ST. This is achieved by communicating the legal source and destination in a two-step process. In the first step, the phase response of the channel is probed, and in the second step, the information-bearing signal is modified to pre-compensate for the phase effects of the channel. As the channels between the legal source and destination are completely different from the channels between the legal source and eavesdroppers, this process is secure [119],[120]. It is assumed that each node carries a single omnidirectional antenna, the relaying strategy is decode-and-forward (DF), and global channel state information (CSI) is available by a standard channel estimation (CE) technique; that is, training-based CE (TBCE). In TBCE, the pilot symbols are used for acquiring an estimated CSI prior to actual data transmission, and subsequently the channel is estimated using the combined knowledge of the transmitted and received signals [122] and [123]. To enhance the achievable secrecy rate, the ST allocates part of its transmitting power to emit a jamming signal and the remainder to emitting the information signal. Depending upon the secrecy capacity of the wiretap channel in [102], the secrecy capacity C_{sec} for input s is given by

$$C_{sec} \;=\; \max_{s}[I(s,x) - I(s,x_{ED})] \geq \max_{s}[I(s,x)]$$

$$- \max_{s}[I(s, x_{ED})], \tag{5.1}$$

where x and x_{ED} are the signals received by the ST and ED, respectively. In this chapter, any pair of mutual information $(I(s,x), I(s,x_{ED}))$ for messages x and x_{ED} is considered to be achievable if the average error probabilities, $P_{e,1} = Pr(\hat{x} \neq x)$ and $P_{e,2} = Pr(x_{\hat{ED}} \neq x_{ED})$, can be made arbitrarily small. The secrecy rate can be defined as

$$\begin{aligned} R_{sec} &= \max_{s}[I(s,x)] - \max_{s}[I(s,x_{ED})] \\ &= (R_D - R_E)^+, \end{aligned} \tag{5.2}$$

where R_D is the information rate at the destination and R_E is the leakage rate at the eavesdropper; and $(x)^+ = \max(0,x)$ to guarantee that the value of the secrecy rate is positive. For convenience, the $(\cdot)^+$ sign is omitted from subsequent expressions.

5.2.1 Proposed cooperative CRNs

The system has three phases:

1) Phase 1: The PT decides to allocate only a fraction $(1-\alpha)$ of the whole time slot for transmission from the PT to the ST (where $0 < \alpha < 1$.). The remaining fraction will be used in Phases 2 and 3. It is assumed that transmission from the PT is invisible at the ED. The PT encodes a confidential message into a $n-$length block codeword (s), with the following power constraint [115]:

$$P_p = \frac{1}{n}\sum_{k=1}^{n} |s_k|^2 \leq P_{MAX}, \tag{5.3}$$

where P_{MAX} is the maximum primary power of the PT. In Phase I, the ST is used as a relay and the received signal at the ST is

$$X_{ST} = \sqrt{P_p} h_{ps} s + n_{ST}, \tag{5.4}$$

where s is the primary message signal, P_p is the primary power level, $n_{ST} \sim \mathcal{CN}(0, \sigma^2)$ is the noise at the ST, and $h_{ps} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient

between the PT and ST. For notational convenience, let us define

$$\rho_{ps} = \frac{P_p \left|h_{ps}\right|^2}{\sigma^2}.$$

Then, the information rate at the ST, R_{PS}, is obtained as

$$R_{PS} = (1-\alpha)\log_2(1+\rho_{ps}). \tag{5.5}$$

2) Phase 2: The ST then forwards the secure primary message to the PR within the fraction $\alpha\beta$ (where $0 < \beta < 1$) of the considered time slot. In this phase, for security reasons, the ST also re-encodes the artificial noise, z, using a faction $(1-\epsilon)$ of the available power level, P_s (where $0 < \epsilon < 1$). Furthermore, the ST encodes a confidential message into the $n-$length block codeword from Phase 1, with the power of the ST constrained by

$$P_s = \frac{1}{n}\sum_{k=1}^{n} \left|\hat{s}_k\right|^2 \leq P_{s,MAX}, \tag{5.6}$$

where $P_{s,MAX}$ is the maximum secondary power of the ST. The received signal at the PR after removing the artificial noise (which is assumed to be known at the PR) is

$$X_{PR} = \sqrt{\epsilon P_s} h_{sp} \hat{s} + n_{PR}, \tag{5.7}$$

and the received signal at the ED in Phase 2 is

$$X_{ED}^{(2)} = \sqrt{\epsilon P_s} h_{se} \hat{s} + \sqrt{(1-\epsilon)P_s} h_{se} z + n_{ED}, \tag{5.8}$$

where $\hat{s}$ is the re-encoded primary message signal, $z \sim \mathcal{CN}(0,1)$ is the artificial noise, $h_{sp} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the ST and the PR, and $h_{se} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the ST and the ED. After removing the artificial noise, the information rate at PR becomes

$$R_{SP} = \alpha\beta \log_2(1+\epsilon\rho_{sp}), \tag{5.9}$$

where

$$\rho_{sp} = \frac{P_s \left|h_{sp}\right|^2}{\sigma^2}.$$

The information leakage at the ED in Phase 2 is then

$$R_{SE}^{(2)} = \alpha\beta \log_2(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}), \tag{5.10}$$

where

$$\rho_{se} = \frac{P_s |h_{se}|^2}{\sigma^2}.$$

Then, the achievable PSR, denoted by R_{psec}, can be written as

$$\begin{aligned} R_{PSEC} &= R_{SP} - R_{SE}^{(2)} \\ &= \alpha\beta(\log_2(1+\epsilon\rho_{sp}) - \\ &\quad \log_2(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})})). \end{aligned} \tag{5.11}$$

3) Phase 3: The ST sends its own secure secondary message to the SR within the remaining fraction $\alpha(1-\beta)$ of the considered time slot. Again the analysis is simplified by assuming that the secondary transmission uses the same codeword for the artificial noise and the same power allocation strategy (i.e., the same ϵ) as previously. The received signal at the SR (after removing the artificial noise) is

$$X_{SR} = \sqrt{\epsilon P_s} h_{ss} s_1 + n_{SR}, \tag{5.12}$$

while the received signal at the ED in Phase 3 is

$$X_{ED}^{(3)} = \sqrt{\epsilon P_s} h_{se} s_1 + \sqrt{(1-\epsilon)P_s} h_{se} z + n_{ED}, \tag{5.13}$$

where s_1 is the secondary message signal and $h_{ss} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the ST and SR. After removing the artificial noise at the SR, the information rate at the SR is represented as

$$R_{SS} = \alpha(1-\beta)\log_2(1+\epsilon\rho_{ss}), \tag{5.14}$$

where

$$\rho_{ss} = \frac{P_s |h_{ss}|^2}{\sigma^2}.$$

Additionally, the leakage rate at the ED in this phase can be written as

$$R_{SE}^{(3)} = \alpha(1-\beta)\log_2(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}). \tag{5.15}$$

Similarly, the SSR, denoted by R_{SSEC}, can be obtained as

$$\begin{aligned} R_{SSEC} &= R_{SS} - R_{SE}^{(3)} \\ &= \alpha(1-\beta)\left(\log_2(1+\epsilon\rho_{ss})\right. \\ &\quad \left. - \log_2\left(\frac{(1+\rho_{se})}{(1+(1-\epsilon)\rho_{se})}\right)\right). \end{aligned} \tag{5.16}$$

5.2.2 Maximisation of achievable secrecy rates using a Stackelberg game

The maximisation problem of available secrecy rates can be formulated as a Stackelberg game wherein the PT is considered the leader and the ST the follower. The leader attempts to maximise its primary secrecy rate, R_{psec}, while the follower attempts to maximise its utility. The optimal transmission parameters for the PT, (α^*, β^*), and the corresponding power choice of the ST, ϵ^*, are jointly referred to as the Stackelberg equilibrium. Figure 6.3 shows the interaction between the primary and secondary transmissions. The ST is aware of parameters (α, β) and optimises

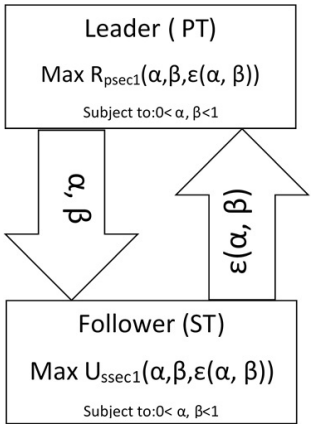

Figure 5.3: Stackelberg game model

its power level towards the goal of maximising its utility:

$$U_{SSEC}(\alpha, \beta, \epsilon(\alpha, \beta)) = R_{SSEC} - k\epsilon, \tag{5.17}$$

where k is the pricing constant. The following lemma is considered.

Lemma 5. *The utility of the secondary transmission in Equation* (6.16) *is concave with respect to* ϵ.

Proof: Please see Appendix 2.A. ■

The optimal solution to the secondary transmission problem can be obtained as

$$\epsilon^* = \arg \max_{0<\alpha,\beta,\epsilon<1} U_{SSEC}(\alpha, \beta, \epsilon(\alpha, \beta)). \tag{5.18}$$

To find the optimum ϵ^*, it is possible to differentiate U_{ssec} with respect to ϵ and equate it to zero:

$$\begin{aligned} \frac{\partial U_{SSEC}}{\partial \epsilon} &= q\left(\frac{\rho_{ss}}{(1+\epsilon\rho_{ss})} - \frac{\rho_{se}}{(1+(1-\epsilon)\rho_{se})}\right) - k = 0 \\ \Rightarrow k/q &= \frac{\rho_{ss}}{(1+\epsilon\rho_{ss})} - \frac{\rho_{se}}{(1+(1-\epsilon)\rho_{se})} \end{aligned} \tag{5.19}$$

After simplification, ϵ is obtained as

$$a\epsilon^2 + b\epsilon + c = 0, \tag{5.20}$$

where

$$a = \rho_{ss}\rho_{se}, \tag{5.21}$$

$$b = \rho_{se} - \rho_{ss} - \rho_{ss}\rho_{se} - \frac{2\rho_{ss}\rho_{se}q}{k}, \tag{5.22}$$

$$c = \frac{q}{c_1}(\rho_{ss} - \rho_{se} + \rho_{ss}\rho_{se}) - \rho_{se} - 1. \tag{5.23}$$

Therefore, the optimal ϵ^* is

$$\epsilon^* = \begin{cases} 0, & \epsilon_2 \leq 0 \\ 1, & \epsilon_1 \leq 1 \\ \max_{\epsilon\in\{\epsilon_1,\epsilon_2\}} U_{ssec}(\epsilon), & 0 \leq \epsilon_1 \leq \epsilon_2 \leq 1 \\ \max_{\epsilon\in\{0,1,\epsilon_i\}} U_{ssec}(\epsilon), & \text{only } \epsilon_i \in [0,1], i = 1 \text{ or } 2 \end{cases} \tag{5.24}$$

where

$$\epsilon_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},\ \epsilon_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

The PT, acting as the game leader, determines the fraction α and the ratio β with the goal of maximising its secrecy rate, knowing that its decision will affect the

strategy selected by the ST (the follower). The solution is

$$\alpha^*, \beta^* = \arg \max_{0<\alpha,\beta,\epsilon<1} R_{PSEC}(\alpha, \beta, \epsilon^*(\alpha, \beta)). \tag{5.25}$$

Theorem 1. *The allocated power level ϵ^* and time slot α^* are the Nash equilibrium of the proposed game.*

Proof: According to the DF scheme, it would be assumed that $R_{sp} \leq R_{ps}$ in order to find the relationship between α and β to facilitate the solution of the above optimization problem. The following relationship can be obtained according to the assumption of the DF scheme:

$$\begin{aligned} R_{SP} &= R_{PS} \\ \Rightarrow \beta &= \frac{(1-\alpha)}{\alpha} \frac{\log_2(1+\rho_{ps})}{\log_2(1+\epsilon\rho_{sp})}. \end{aligned} \tag{5.26}$$

According to Lemma 1, U_{SSEC} is strictly concave in terms of ϵ for a given values of α and β. Furthermore, if R_{PSEC} is an increasing function of α, then the primary transmission (leader) will select the best response $\epsilon^*(\alpha)$ of the secondary transmission (follower) as

$$\alpha^* = \arg\max R_{PSEC}(\alpha, \epsilon^*(\alpha)). \tag{5.27}$$

Therefore, α^* and $\epsilon^*(\alpha^*)$ form the Nash equilibrium of the proposed Stackelberg game. ■

5.3 Extension to multiple eavesdroppers (Scenario II)

Scenario II (see Figure 6.2) is considered by having multiple eavesdroppers which are located in the range of the ST to highlight their effect on the secrecy rates. In this case, it cannot be assumed that all eavesdroppers are located out of range of the PT, as was possible in Scenario 1. Instead, to enhance the secure transmission, the SR is considered as a jammer with multiple transmission antennas, and suppose

that it transmits a jamming signal in Phase 1. The three phases are considered in the cases of colluding and non-colluding eavesdroppers, and closed-form expressions are derived for both the PSR and SSR in each case.

5.3.1 Case I: colluding eavesdroppers

In this case, all eavesdroppers cooperate via central processing such that they can be considered as a single eavesdropper with multiple antennas. We assume that the eavesdroppers are homogeneous; that is, each eavesdropper experiences the same received signal power on average. Moreover, all eavesdroppers are uniformly located around a legitimate ST [106].

1) Phase 1: The PT is considered to cooperate with the ST by allocating only a fraction $(1-\alpha)$ of the whole time slot, whereas the SR, with multiple transmitting antennas, sends the jamming signal using power vector $\mathbf{w}_J$ to both the ST and ED within the fraction $(1-\alpha)$. In this phase, the received signal, X_{ST}, at the ST is

$$X_{ST} = \sqrt{P_p} h_{ps} s + \sqrt{P_J} \mathbf{h}_{rs} \mathbf{w}_J z_J + n_{ST}, \tag{5.28}$$

where $\mathbf{h}_{(rs)} \sim \mathcal{N}(\mathbf{0}_K, d^{-\delta}\mathbf{I}_K)$ is the channel vector (of length K due to K multiple transmit antennas at the SR) between the SR and ST, $z_J \sim \mathcal{CN}(0,1)$, δ is the path loss exponent, d is the distance between the SR and ST, and $n_{ST} \sim \mathcal{CN}(0,\sigma^2)$. The received signal at the ED_i (with $i = 1, 2, ..N$) in Phase 1 is

$$X_{PE,i} = \sqrt{P_p} h_{pe} s + \sqrt{P_J} \mathbf{h}_{re} \mathbf{w}_J z_J + n_{ED,i}, \tag{5.29}$$

where $\mathbf{h}_{(re)} \sim \mathcal{N}(\mathbf{0}_K, d^{-\delta}\mathbf{I}_K)$ is the channel vector (of length K due to K multiple transmit antennas at the SR) between the SR and ST, and $n_{ED,i} \sim \mathcal{CN}(0,\sigma^2)$. Using projection matrix theory to remove an interference of the SR (the jammer) in the legal receiver (the ST) , $|\mathbf{w}_J|$ can be achieved as follows:

$$|\mathbf{w}_J| = \frac{(\mathbf{I} - \mathbf{h}_{rs}(\mathbf{h}_{rs}{\mathbf{h}_{rs}}^{\dagger})^{-1}\mathbf{h}_{rs}^{\dagger})\mathbf{h}_{re}}{\left|((\mathbf{I} - \mathbf{h}_{rs}(\mathbf{h}_{rs}{\mathbf{h}_{rs}}^{\dagger})^{-1}\mathbf{h}_{rs}^{\dagger})\mathbf{h}_{re}\right|}, \tag{5.30}$$

where $|\mathbf{w}_J {\mathbf{w}_J}^{\dagger}| = 1$.

Therefore, the information rate at the ST is is given by Equation (6.3), while the leakage rate at ED_i can be written as

$$R_{PE,i} = (1-\alpha)\log_2\left(1+\frac{P_p h_{pe}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{w}_J\mathbf{h}_{re}\right|}\right), \tag{5.31}$$

where $\mathbf{W}_J = \mathbf{w}_J\mathbf{w}_J{}^{\dagger}$.

2) Phase 2: The ST has a DF relay function and forwards the secure primary message, $\hat{s}$, to the PR in $\alpha\beta$ in the presence of L eavesdroppers according to a parameter $0 < \beta < 1$. The received signal, X_{PR}, and rate, R_{SP}, are given by Equation (6.41) and Equation (6.42), respectively, due to cancelling of artificial noise in the PR. The leakage rate, R_{SEi}, at the i^{th} ED can then be written as

$$R_{SE,i} = \alpha\beta\log_2(1+\frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{w}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}}), \tag{5.32}$$

where $h_{se} \sim \mathcal{CN}(0,\sigma_h^2)$ is the channel coefficient between the ST and the i^{th} ED. In [106] and [121], the authors took the sum of the signal-to-interference-and-noise ratio ($SINR$)s of the colluding eavesdroppers due to their cooperation. In this chapter, assuming sequential Markov chain observations of the eavesdroppers and, following [118], it is possible to utilise $(\sum_{i=1}^{L} log2(1+SINR_i)) \cong \sum_{i=1}^{L} SINR_i$, considering the approximation $(log2(1+SINR_i)) \cong SINR_i$ for long-distance transmissions or energy-limited scenarios. This assumption represents the worst case for eavesdroppers ($i.e.(\sum_{i=1}^{L} log2(1+SINR_i) > log2(1+\sum_{i=1}^{L} SINR_i))$). Therefore, R_{SE} is rewritten as

$$\begin{aligned} R_{SE} &= \sum_{i=1}^{L} R_{SE,i}{}^{(2)} \\ &= \sum_{i=1}^{L} \alpha\beta\left(\log_2(1+\frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + \frac{}{(1-\epsilon)P_s h_{se}})}\right). \end{aligned} \tag{5.33}$$

Moreover, the information rate, R_P, at the PR is

$$R_P = \min(R_{PS}, R_{SP})$$

$$= \min\left(\log_2(1+\rho_{ps}), \log_2(1+\epsilon\rho_{sp})\right). \quad (5.34)$$

The achievable primary secrecy rate, R_{PSEC}, can then be written as

$$R_{PSEC} = \alpha\beta\left(R_p - \sum_{i=1}^{L}\log_2(1+\frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + \frac{}{(1-\epsilon)P_s h_{se}}})\right). \quad (5.35)$$

2) Phase 3: The ST transmits a secondary message to the SR in time slot $\alpha(1-\beta)$ in the presence of L eavesdroppers. The SR extracts only the information signal, and the information rate at the SR is given by Equation (5.14), while the rate at multiple eavesdroppers is given by

$$R_{SE}{}^{(3)} = \sum_{i=1}^{L}(\alpha(1-\beta)(\log_2(1+\frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}})\Bigg). \quad (5.36)$$

The secondary secrecy rate, R_{SSEC}, can be obtained by substituting R_{ss} and R_{se} such that

$$\begin{aligned} U_{SSEC} &= R_{SSEC} - k\epsilon = R_{SS} - R_{SE}^{(3)} - k\epsilon \\ &= \alpha(1-\beta)(\log_2(1+\epsilon\rho_{ss}) \\ &\quad - \sum_{i=1}^{L}(\alpha(1-\beta)\left(\log_2(1+\right. \\ &\quad \left.\frac{\epsilon P_s h_{se}}{\sigma^2 + P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}})\right) \\ &\quad - k\epsilon. \end{aligned} \quad (5.37)$$

Lemma 6. *The utility of secondary transmission in colluding eavesdroppers distributed uniformly around the legal transmitter is concave with respect to ϵ.*

Proof: Please see Appendix 2.B. ■

The interaction between the primary and secondary transmissions shown in Figure 6.3 is considered. This case reflects the impact of L eavesdroppers on the PSR and SSR. To find the optimum ϵ^*, U_{SSEC} can be differentiated with respect to ϵ. Assuming $\rho_{re} = \frac{P_J \left|\mathbf{h}_{re}^{\dagger} \mathbf{W}_J \mathbf{h}_{re}\right|}{\sigma^2}$ for simplicity, the optimal ϵ^* is one of the positive real roots of $a\epsilon^2 + b\epsilon + c = 0$, where a, b and c are given by

$$a = \rho_{ss}\rho_{se}, \tag{5.38}$$

$$b = \rho_{se} - \rho_{ss} - \rho_{ss}\rho_{se} - \rho_{ss}\rho_{re}, - \frac{(1+L)\rho_{ss}\rho_{se}q}{k} \tag{5.39}$$

$$c = \frac{q}{c_1}(\rho_{ss} - L\rho_{se} + \rho_{ss}\rho_{se} + \rho_{ss}\rho_{re}) - \rho_{se} - 1 - \rho_{re}. \tag{5.40}$$

Theorem 1 can then be applied to find the optimum values of (α, β).

5.3.2 Case 2: non-colluding eavesdroppers

A non-homogeneous distribution of all eavesdroppers around the ST will be considered; that is, the eavesdroppers are distributed randomly with different distances around the ST. In this case, each eavesdropper will have its own information rate, denoted by $R_{se,i}$, $i = 1, 2, \cdots, L$. Thus, the two following problems are formulated:

1) Problem 1: Maximising the PSR in Phase 2 for its worst-case scenario:

$$\max_{0<\alpha,\beta,\epsilon<1} \min_i R_{psec,i} \tag{5.41}$$

where $i = 1, 2, .., L$, $R_{psec,i} = R_{ps} - R_{se,i}$, and $R_{se,i}^{(2)}$ is the leakage rate of the ith ED in Phase 2. Note that

$$\min_i R_{psec,i} = R_{ps} - \max_i R_{se,i}^{(2)}.$$

2) Problem 2: Maximising the SSR in Phase 3 for its worst case scenario:

$$\max_{0<\alpha,\beta,\epsilon<1} \min_i R_{ssec,i} \tag{5.42}$$

where $R_{ssec,i} = R_{ss} - R_{se,i}^{(3)}$ and $R_{se,i}^{(3)}$ is the leakage rate of the ith ED in Phase 3. Similarly, it is the case that

$$\min_i R_{ssec,i} = R_{ss} - \max_i R_{se,i}^{(3)}.$$

To solve the aforementioned two problems, each problem can be decomposed into L independent subproblems, with the i^{th} subproblem is corresponding to the i^{th} eavesdropper. The Stackelberg game-based algorithm proposed in Scenario I can then be applied for the i^{th} eavesdropper to find the suboptimal values of α, β, and ϵ.

5.4 Results and discussion

In this section, numerical results and related discussion are presented. The two optimisation problems from the previous sections are considered according to the Stackelberg game, and examine the secrecy performance under two scenarios.

5.4.1 Scenario I: comparison with previous work

This section compares our proposed system with a jammer that has caused an interference in the legal receiver, as in [99]. The same setting used in this previous study is considered: P_s=2mw, noise variance σ^2 =1mw, pricing factor $k = 0.01$, $|h_{ps}|^2 = 0.6$, $|h_{se}|^2 = 0.3$ and $|h_{ss}|^2 = 0.8$. In [99], the authors considered two secondary users (one for the relay and another for the jammer) in order to enhance the secrecy rates in the primary transmission of the CR. Two schemes represented a relay non-friendly jammer (R-J) and an equal-duration relay non-friendly jammer (EDRJ). Note that the only difference between EDRJ and R-J schemes is that in an EDRJ scheme, the time durations for the first two phases are equal and the secrecy rate is maximized without considering the time allocation. The proposed scheme is now compared with these two schemes. Figure 5.6 indicates that the proposed system outperforms the R-J and EDRJ schemes significantly due to removal of interference from the jamming signal at legal destinations.

Figure 5.7 shows a comparison between the proposed system and equal-duration relay jammer transmissions (EDJ) with respect to h_{se}. The EDJ scheme treats the SR as a potential eavesdropper with respect to the primary transmission. Since the primary users are the legacy owners of the spectrum, the confidentiality of the primary message should be considered. In this context, the PT may be assisted by the trustworthy ST if such cooperation can improve the secrecy performance, with the ST awarded a share of the spectrum for its data transmission. Hence, the ST acts as a friendly jammer and the time durations of the primary and jammer transmissions are the same. This scheme is similar to the jammer in [98], except that the EDJ does not cause an interference with the legal transmitter. This comparison highlights the effect of an interaction between the time and power allocation by the Stackelberg game on a balance-performing process between maximum values for both the primary and secondary secrecy rates. It is notable that the proposed system has a slightly lower primary secrecy rate than the friendly jammer, particularly in the case of a high channel coefficient between the legitimate transmitter and eavesdropper. In contrast, the secondary secrecy rate of the proposed system is significantly higher than that of the friendly jammer. Moreover, the proposed system has a less significant gap between the primary and secondary secrecy rates than the EDJ scheme. Consequently, the PSR and SSR of the Stackelberg game are fairer than those of the EDJ, due to the tradeoff between allocated power, ϵ, and time durations, α and β, in obtaining maximum values for the primary and secondary secrecy rates.

5.4.2 Fixed locations of the PR, ST and SR

The PR, ST and SR locations are fixed at the coordinates (0, 0.6), (0, 0), and (0, 0.4), respectively, to find the effect of PT and ED distances on the PSR and SSR. These coordinates are normalised to a square area with 1km^2. Te path loss model $h_{ij} = d^{-\delta}$ with path loss exponent $\delta = 3$ is applied. The primary and secondary signal-to-noise ratios (SNRs) are set to 5 dB and the pricing coefficient to $k = 0.25$.

Figure 6.6 indicates the optimum primary and secondary secrecy rates with respect to the distance between the PT and ST when the coordinates of the ED are fixed at (1, 0). Notably, the optimum secrecy rates of both the primary and secondary transmissions decrease when the PT is farther away from the ST. This is because a decreasing ρ_{ps} reduces R_{ps} according to Equation (6.3). Hence, the information rate of the relay ST decreases according to the condition $R_{sp} \leq R_{ps}$.

Figure 6.7 shows the optimum PSR and SSR with respect to distance of the ED when the location of the PT is fixed at (0.2, 0). The optimum secrecy rates of both the primary and secondary transmissions increase when the ED is further away from the ST because the information rate of the ED decreases with degradation of h_{se} according to Equation (6.8) and Equation (6.31).

Figure 5.10 shows the optimum ϵ (power level fraction of the ST carrying the message signal) with respect to the distance between the PT and ST when the coordinates of the ED are fixed at (1.0, 0). It is found that the optimum ϵ decreases when the PT is far away from the ST, because the received power at the ST decreases with increasing distance between the ED and ST. This figure also shows the optimum ϵ versus the distance between the ED and ST when the coordinates of the PT are fixed at (0,0.2). In this case the optimum ϵ increases when the ED is farther from the ST because $(1 - \epsilon^*)$ decreases with the decreasing information rate of the ED.

Figure 5.11 shows the optimum α and β versus the distance between the PT and ST when the coordinates of the ED are fixed at (1.0,0). It is found that β^* changes slightly with distance, whereas α^* decreases significantly with distance for two reasons. First, the activation time for transmission between the PT and the relay is independent of β^*, according to Equation (6.3); and secondly, the activation time for transmission between the relay ST and PR decreases with increasing $(1-\alpha^*)$ (the time slot for transmission between the PT and relay) due to the degradation of h_{ps} and R_{ps} according to Equation (6.3).

Figure 5.12 shows the optimum α and β against the distance between the ED and ST when the coordinates of the PT are (0,0.2). Here, β^* is reduced significantly

because h_{se} has its main effect on the relay and secondary transmissions in Phase 2 ($\beta^*\alpha^*$) and Phase 3 $\alpha^*(1-\beta^*)$ according to Equation (6.8) and Equation (6.31), respectively. Additionally, α^* decreases less significantly because h_{se} has no effect on Phase 1 $(1-\alpha^*)$ of the primary transmission, as a result of our assumption that the primary transmission is invisible at the ED.

5.4.3 Fixed locations of the PT, PR, ST and SR

The locations of the PT, PR, ST, and SR are fixed at the coordinates (0,0.2),(0.6, 0), (0, 0), and (0, 0.4), respectively, in order to determine the effect of ρ_{sp} on the secrecy rates in the two later phases. Three schemes are considered depending on the locations of the ED: Scheme I (1.0,0), Scheme II (0.9,0), and Scheme III (0.6,0). Figures 5.13 and 5.14 show the optimum primary and secondary secrecy rates with respect to ρ_{sp} in these three schemes. For all three schemes, the optimum secrecy rates increase significantly with ρ_{sp} according to Equation (6.8) and Equation (6.31).

5.4.4 Scenario II

The same locations and parameters as in the preceding subsection are now considered, but with K=2. Figures 5.15 and 5.16 show that the primary and secondary secrecy rates decrease significantly in both cases with an increasing number of eavesdroppers, according to Equation (6.23) and Equation (B.2). Moreover, Scheme II (with non-colluding eavesdroppers) has a secrecy rate higher than that of Scheme I (with colluding eavesdroppers) because Scheme I combines the effects of all eavesdroppers, while Scheme II selects the worst response (minimum secrecy rate) from one of the eavesdroppers.

Figure 5.17 shows that ϵ^* decreases significantly with an increasing number of eavesdroppers, because more power should be allocated to the artificial noise as the number of eavesdroppers grows. Additionally, ϵ^* reaches a higher level when the distance between the ST and ED increases, due to the fact that less power should be allocated to the artificial noise if R_{es1} is reduced.

Figure 5.18 shows that α^* increases significantly with an increasing number of eavesdroppers, because the activation time of Phases II and III must be increased to maintain reasonable values for the secrecy rates with more eavesdroppers. Furthermore, α^* must increase with larger distances between the ST and ED.

5.5 Part II: physical layer security via a multi-level Stackelberg game

The aforementioned studies focused on enhancing the primary secrecy rate and the secondary transmission rate, under the assumption that the eavesdropper can intercept the primary transmission only. Inspired by the study in [**?**], a new scenario is proposed wherein the PT allows the ST to access its spectrum for better secrecy performance. It is assumed that the ED can intercept both the primary and secondary transmissions in the worst case, and the ST is used as a trusted relay and jammer for primary transmission. It is also assumed that the PT and ST can allocate some of their transmission power to transmit artificial noise and thereby create interference at the ED. In such networks, a primary user may lease portions of a licensed spectrum to a secondary user in exchange for enhanced performance. This scenario avoids the regulatory issues or money transactions that commonly hinder the implementation of the property-rights spectrum leasing concept. The main contributions of this work are:

- A resource allocation scheme (i.e., power and time resources) is proposed for spectrum leasing to maximise the primary secrecy rate (PSR), relay secrecy rate (RSR), and secondary secrecy rate (SSR) with perfect knowledge of channel state information (CSI).

- The unique value of the proposed Stackelberg game equilibrium is obtained.

- It is shown that the secrecy rate of the proposed system using a multi-level Stackelberg game is significantly higher than that using the single level

Stackelberg game..

- Comparisons with previous work are provided to show the significant improvement to security in the proposed system.

5.6 System models

Similarly to the problems considered previously, the CRN consists of the following single-antenna nodes: a primary transmitter (PT), a cognitive secondary transmitter (ST), a primary receiver (PR), a secondary receiver (SR), and an eavesdropper (ED) (Figure 5.4). A CRN is considered wherein a ST transmits to a SR using the spectrum between a PT and a PR under malicious attempts by an ED. It is assumed that each node carries a single omnidirectional antenna, the relaying strategy is decode-and-forward (DF), and the global channel state information (CSI) is available by a standard channel estimation (CE) technique, the training-based CE (TBCE). There is no extra jammer, but *a priori* knowledge of jamming signals is available at legitimate receivers. This is achieved by communication of a key for artificial noise between the legal source and destination [119, 120]. To enhance secrecy rates, the legitimate transmitters are permitted to use a portion of their power to transmit a jamming signal, in addition to transmitting the message signal.

We have three phases for transmissions: the primary secrecy rate in Phase I (PSR), the relay secrecy rate in Phase II (RSR), and the secondary secrecy rate in Phase III (SSR). Since the ED can intercept the primary, relay, and secondary transmissions in three phases, our objective is to improve the secrecy rates in all three via transmission of appropriate jamming signals.

Phase 1: Using a fraction of the considered time slot $(1-\alpha)$, where $0 < \alpha < 1$, the PT sends its message signal and the ST acts as the relay to receive as follows:

$$x_{ST} = \sqrt{\epsilon_1 P_p} h_{ps} s_1 + \sqrt{(1-\epsilon_1) P_p} h_{ps} z_1 + n_{ST}, \tag{5.43}$$

where s_1 is the message signal, z_1 is artificial noise, $n_{ST} \sim \mathcal{CN}(0, \sigma^2)$ is the noise at the ST, ϵ_1 is the PT's allocated power for transmission of the primary message,

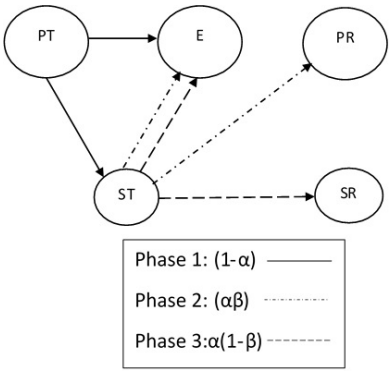

Figure 5.4: Illustration of the CR system model

and $h_{ps} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the primary and secondary transmitter. For notational convenience, let us define

$$\rho_{ps} = \frac{P_p \left|h_{ps}\right|^2}{\sigma^2}.$$

It is assumed that the ST has *a priori* knowledge of the artificial noise. The achievable secrecy rate R_{PSR} in Phase I can be calculated as follows:

$$R_{PSR} = R_{ps} - R_{pe}, \tag{5.44}$$

$$R_{PSR} = (1-\alpha)\left[\log_2(1+\epsilon_1\rho_{ps}) - \log_2(\frac{(1+\rho_{pe})}{(1+(1-\epsilon_1)\rho_{se})})\right]. \tag{5.45}$$

Phase 2: The ST functions as a trusted relay to forward a secure primary message, X_{ST}, to the PR in time slot $\alpha\beta$ with $0 < \alpha, \beta < 1$. It holds that

$$X_{PR} = \sqrt{\epsilon_2 P_s} h_{sp} \hat{s_1} + \sqrt{(1-\epsilon_2)P_s} h_{sp} z_2 + n_{PR}, \tag{5.46}$$

where $\hat{s_1}$ is the re-encoded message signal, z_2 is artificial noise, ϵ_2 is the power allocated to the ST for relaying the primary message, and $h_{sp} \sim \mathcal{CN}(0, \sigma_h^2)$ is the channel coefficient between the secondary transmitter and primary receiver. After removing the artificial noise at the primary receiver, the achievable secrecy rate in Phase II, R_{RPR}, becomes

$$R_{RPR} = R_{sp} - R_{se}, \tag{5.47}$$

$$R_{RPR} \quad = \quad (\alpha\beta)\left[\log_2(1+\epsilon_2\rho_{sp})\right.$$

$$-\log_2(\frac{(1+\rho_{se}+(1-\epsilon_1)\rho_{pe})}{(1+(1-\epsilon_2)\rho_{se}+(1-\epsilon_1)\rho_{pe})})\Big], \tag{5.48}$$

where

$$\rho_{sp} = \frac{P_s\left|h_{sp}\right|^2}{\sigma^2},$$

and

$$\rho_{se} = \frac{P_s\left|h_{se}\right|^2}{\sigma^2}.$$

Phase 3: The ST sends secure secondary message to the SR in time slot $\alpha(1-\beta)$. The received secondary message, X_{SR}, can be written as

$$X_{SR} = \sqrt{\epsilon_2 P_s}h_{ss}s_2 + \sqrt{(1-\epsilon_2)P_s}h_{ss}z_2 + n_{SR}, \tag{5.49}$$

where s_2 is the secondary message signal and $h_{ss} \sim \mathcal{CN}(0,\sigma_h^2)$ is the channel coefficient between the secondary transmitter and receiver. It is assumed that the same codewords for artificial noise are used in the primary and secondary transmissions. After removing the artificial noise at the secondary receiver, the following secrecy rate is obtained in Phase III R_{SSR}:

$$R_{SSR} = R_{ss} - R_{se}, \tag{5.50}$$

$$\begin{aligned} R_{SSR} &= \alpha(1-\beta)\left[\log_2(1+\epsilon_2\rho_{ss})\right. \\ &\quad \left. -\log_2(\frac{1+\rho_{se}+(1-\epsilon_1)\rho_{pe}}{1+(1-\epsilon_2)\rho_{se}+(1-\epsilon_1)\rho_{pe}})\right], \end{aligned} \tag{5.51}$$

where

$$\rho_{ss} = \frac{P_s\left|h_{ss}\right|^2}{\sigma^2}.$$

5.7 A secrecy rate measure and game-theoretic model

Throughout this section, the nodes are defined as selfish and rational to capture non-altruistic behaviour. An appropriate framework for analysing the interaction between such nodes is a multi-level Stackelberg game. If this game includes M

players with N levels, then the lth player is the follower of the $(l-1)$th player at the ith level and is a leader of the $(l+1)$th player at the $(i+1)$th level, where $1 < i < N$ and $1 < l < M$. Furthermore, the first player is the leader at the first level and the Mth player is the follower at the Nth level. In general, the number of levels is equal to the number of players minus one (i.e., $N = M - 1$). Hence, two levels of the Stackelberg game are applied (Figure 5.5) to maximise the secrecy rates in the three phases, which are our players.

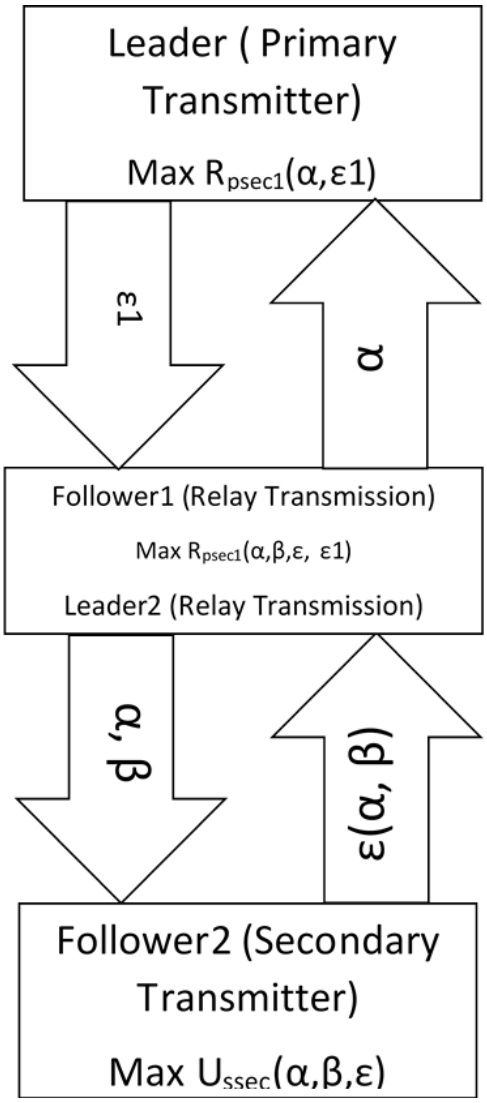

Figure 5.5: A two-level Stackelberg game for the proposed system

5.7.1 Level 1

The leader and follower are the PT and relay transmissions, respectively. The optimal value ϵ_1^* can be represented as

$$\epsilon_1^* = \arg\max R_{PSR}(\alpha, \epsilon_1). \tag{5.52}$$

Lemma 7. *The secrecy rate at Phase I in Equation* (6.7) *is concave in terms of* ϵ_1.

Proof: In order to prove the concavity of the primary transmission's utility, the second derivative of Equation (6.7) is taken with respect to ϵ_1:

$$\begin{aligned} \frac{\partial^2 R_{PSR}}{\partial^2 \epsilon_1} &= q_1 \left[(-\frac{\rho_{ps}^2}{(1+\epsilon_1\rho_{ps})^2} \right. \\ &\quad \left. -\frac{\rho_{pe}^2}{(1+(1-\epsilon_1)\rho_{pe})^2}) \right], \end{aligned} \tag{5.53}$$

where $q_1 = (1-\alpha)/\ln 2$. As this second derivative is negative, the secrecy rate in Phase I is concave with respect to ϵ_1. ■

According to Lemma 1, ϵ_1^* can be found from solving the following equation:

$$\begin{aligned} \frac{\partial R_{PSR}}{\partial \epsilon_1} &= q_1 \left[\frac{\rho_{ps}}{(1+\epsilon_1\rho_{ps})} \right. \\ &\quad \left. -\frac{\rho_{pe}}{(1+(1-\epsilon_1)\rho_{pe})} \right] = 0, \end{aligned} \tag{5.54}$$

and from Equation (C.5), it is derived that

$$\epsilon_1^* = \frac{\rho_{ps} - \rho_{pe} + \rho_{ps}\rho_{pe}}{2\rho_{ps}\rho_{pe}}. \tag{5.55}$$

5.7.2 Level 2

At the second level, the leader and follower are the relay and the secondary transmissions, respectively. The optimal primary strategy, ϵ_1^* , relay transmitter strategy, (α^*, β^*), and the corresponding power choice of the secondary transmitter, ${\epsilon_2}^*$, comprise the Stackelberg equilibrium. Interactions between the transmissions

in the three phases are shown in Figure 6.2. The ST is aware of parameters (α, β) and optimises its power level with the goal of maximising its utility:

$$U_{ssec}(\alpha, \beta, \epsilon_1^*, \epsilon_2(\alpha, \beta)) = R_{SSR} - k\epsilon_2, \tag{5.56}$$

where k is a pricing constant. Again according to Lemma 1, the utility of the secondary transmission in Equation (6.14) is concave in terms of ϵ_2. The optimal solution of secondary transmission problem can be derived as

$${\epsilon_2}^* = \arg\max U_{ssec}(\alpha, \beta, \epsilon_1^*, \epsilon_2(\alpha, \beta)), \tag{5.57}$$

subject to $0 < \alpha < 1$, $0 < \beta < 1$, and $0 < \epsilon_2 < 1$. To find the optimum ${\epsilon_2}^*$, U_{ssec} can be differentiated with respect to ϵ_2 and equated to zero. After simplification, ϵ_2 is obtained as follows:

$$a{{\epsilon_2}^*}^2 + b\epsilon_2 + c = 0, \tag{5.58}$$

where

$$\begin{aligned} a &= \rho_{ss}\rho_{se}, && (5.59)\\ b &= \rho_{se} - \rho_{ss} - \rho_{ss}\rho_{se} - \rho_{ss}\rho_{pe}(1 - {\epsilon_1}^*) && (5.60)\\ &\quad - \frac{2\rho_{ss}\rho_{se}q}{k}, && (5.61)\\ c &= \frac{q}{k}(\rho_{ss} - \rho_{se} + \rho_{ss}\rho_{se} + \rho_{ss}\rho_{pe}(1 - {\epsilon_1}^*)) && (5.62)\\ &\quad - \rho_{se} - 1 - \rho_{pe}(1 - {\epsilon_1}^*). && (5.63) \end{aligned}$$

The roots $\epsilon_2^{*(1)}$ and $\epsilon_2^{*(2)}$ can then be obtained.

The relay transmission determines the fractions α and β with the goal of maximising its secrecy rate, knowing that its decision will affect the strategy selected by the ST:

$$\alpha^*, \beta^* = \arg \max_{0<\alpha,\beta,\epsilon_1,\epsilon_2<1} R_{RPR}(\alpha, \beta, {\epsilon_1}^*, {\epsilon_2}^*(\alpha, \beta)). \tag{5.64}$$

Theorem 2. *The allocated power levels, $\epsilon_1^*, \epsilon_2^*$, and time slot, α^*, are the Nash equilibrium of the proposed game.*

Proof: According to the DF scheme, it is assumed that $R_{sp} \leq R_{ps}$ in order to find the relationship between α and β to facilitate the solution of the above optimisation problem:

$$\begin{aligned} R_{SP} &= R_{PS} \\ \Rightarrow \beta &= \frac{(1-\alpha)}{\alpha} \frac{\log_2(1+\rho_{ps})}{\log_2(1+\epsilon\rho_{sp})}. \end{aligned} \tag{5.65}$$

According to Lemma 1 in Phases 1 and 3, R_{PSR} and U_{ssec} are strictly concave in terms of ϵ_1 and ϵ_2 for given values of α and β. Furthermore, if R_{RSR} is an increasing function of α, then the relay transmission (leader) in Level 2 will select the best responses, ϵ_1^* of the leader in Level 1 and $\epsilon_2^*(\alpha)$ of the follower in Level 2, as follows:

$$\alpha^* = \arg\max R_{PSEC}(\alpha, \epsilon_1^*, \epsilon_2^*(\alpha)). \tag{5.66}$$

Therefore, α^*, ϵ_1^*, and $\epsilon_2^*(\alpha^*)$ form the Nash equilibrium of the proposed Stackelberg game. ■

Lemma 8. *The Stackelberg game has a higher secrecy rate with N levels than with N-1 levels.*

Proof: $N = 2$ is considered in order to make a direct comparison between a single- and two-level Stackelberg game. In the single level, it is assumed that that the PT is out of range of the eavesdropper to remove the impact of the primary transmitter (the leader in Level 1), which is represented by ϵ_1. In this case, the single level of the Stackelberg game is needed between the relay transmission (leader) and secondary transmission (follower). Following the procedure that was used for Phases 2 and 3 in the study of the multi-level Stackelberg game, the primary secrecy rate, ${R_{RPR}}^{(1)}$, is found:

$$\begin{aligned} {R_{RPR}}^{(1)} &= R_{sp} - {R_{se}}^{(2)} \\ &= \alpha\beta \left[\log_2(1+\epsilon_2\rho_{sp}) \right. \\ &\quad \left. -\log_2(\frac{(1+\rho_{se})}{(1+(1-\epsilon_2)\rho_{se})})\right]. \end{aligned} \tag{5.67}$$

To highlight the enhancement of the primary secrecy rate by the two-level Stackelberg game, it is necessary to prove that

$$R_{RPR} - R_{RPR}{}^{(1)} > 0. \tag{5.68}$$

Since R_{sp} is same in both the single-level and two-level Stackelberg game, it is possible to obtain

$$\begin{aligned} \frac{\epsilon_2 \rho_{sp}}{(1+(1-\epsilon_2)\rho_{se})} \quad &> \quad \frac{\epsilon_2 \rho_{sp}}{(1+(1-\epsilon_2)\rho_{se}+(1-\epsilon_1)\rho_{pe})} \\ &\rightarrow \rho_{pe}(1-\epsilon_1) > 0. \end{aligned} \tag{5.69}$$

■

5.8 Numerical results

This section presents numerical results and some related discussions. Two optimisation problems from the previous section are considered according to the Stackelberg game. Our simulation consists of two steps. Firstly, the following parameters are considered to provide the same setting as in a previous study [99]: $P_s = 2mw$, noise variance $\sigma^2 = 1mw$, pricing factor $c_1 = 0.25$, $|H_{ps}|^2 = 0.6$, $|H_{se}|^2 = 0.3$, and $|H_{ss}|^2 = 0.8$. Figure 5.19 shows a comparison of our proposed scenario with the previous study, which used one secondary user for relay and a second one as a non-friendly jammer. In [99], the authors proposed relay-and-jammer (R-J) and equal-duration relay jammer (EDRJ) schemes to the enhance secrecy rate in the CR. In Figure 5.19, the secrecy rate is plotted versus the channel gain between the legitimate source and destination, (H_{SD}). As before, our proposed system outperforms the R-J and EDRJ schemes significantly, due to its removal of artificial noise, and hence interference, from the legal receiver, and its increase in interference at the eavesdropper due to the interaction between the two levels of the Stackelberg game.

To determine the effect of the signal-to-noise ratio on the secrecy rates in three phases, we fix the locations of the PT, PR, ST, ED, and SR at the coordinates

(0.2,0),(0.6, 0), (0, 0),(0,1), and (0, 0.4), respectively, the path loss model $H_{ij} = d^{-\delta}$ is assumed with path loss exponent $\delta = 3.0$ and the pricing coefficient $k = 0.25$. Figure 5.20 visualises the optimum optimum primary single-level and two-level secrecy rates versus the SNR. It is notable that the primary secrecy rate is improved by the multi-level Stackelberg game according to Lemma 2. Furthermore, the primary secrecy rate of the two-level Stackelberg game increases more significantly than that of the single level, due to the residual effect of ρ_{ps} on the two-level secrecy according to Equation (6.12).

Finally, a scenario is considered in which the PT, ST, SR, and ED have the same locations as in Figure 5.20, but the PR is in a different location, to determine the effect of the destination location on the primary and secondary power allocations and time allocations. Figure 5.21 shows the optimum PSR, RSR, and SSR versus the SNR. Notably, the optimum secrecy rates of all three phases increase significantly with the increasing SNR, due to the increased ρ_{ps}, ρ_{sp}, and ρ_{ss}, respectively.

5.9 Conclusions

In this chapter, a game theory-based cooperation method has been proposed to optimise the primary secrecy rate and secondary secrecy rate in CRNs. This mechanism is built upon the spectrum leasing paradigm, wherein a secondary transmitter is permitted to use some of its own power level to transmit artificial noise to the destination(s) and the legitimate destination has prior knowledge of this artificial noise. Interaction between the cooperative nodes is based on the Stackelberg game concept. Two scenarios have been considered, one with a single eavesdropper and one with multiple eavesdroppers, wherein optimisation problems were formatted and solved in each scheme with the aim of maximising the achievable secrecy rates on the primary and secondary transmissions, subject to constraints on the allocated power and leased time slots. Numerical results have confirmed that our proposed cooperative scheme significantly improves the secrecy rates of the CRNs. Furthermore, it has been observed numerically that the achievable PSR and SSR

of the Stackelberg game is fairer than those of other algorithms in the literature, due to the tradeoff between the allocated power and the time slot durations in the Stackelberg game. Moreover, two levels of Stackelberg game-based cooperation have been proposed to to optimize the physical layer security of both primary and secondary transmissions in CRNs. A constrained optimisation problem has been formulated and solved to maximise the achievable secrecy rates on the primary, relay, and secondary transmissions, again subject to constraints on power allocation and time slots. Numerical results have confirmed that our proposed cooperative scheme significantly improves the primary and secondary secrecy rates of CRNs.

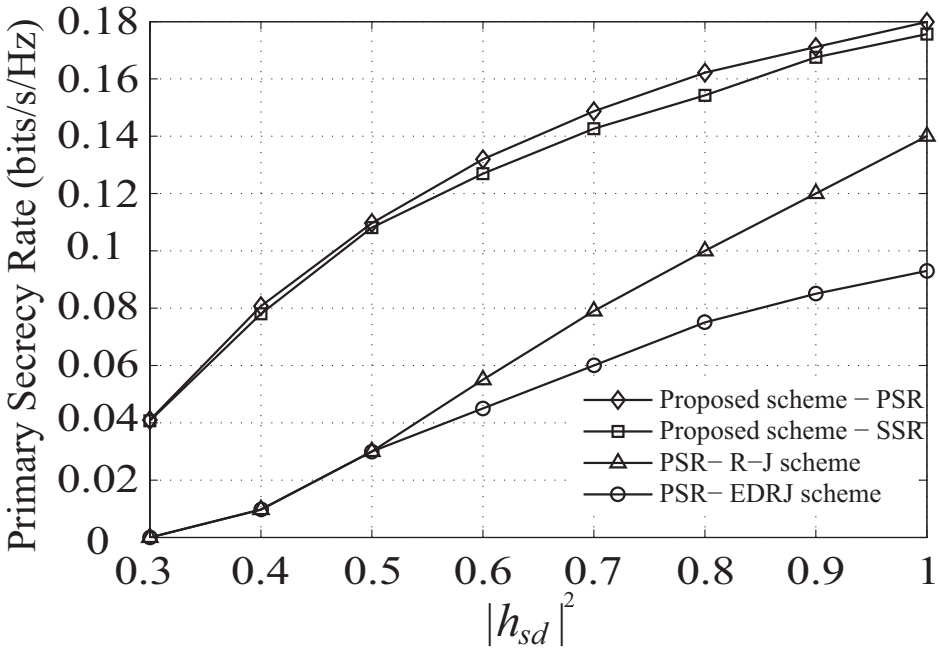

Figure 5.6: Secrecy rate: comparison with jammer-caused interference at the approach to the legitimate receiver

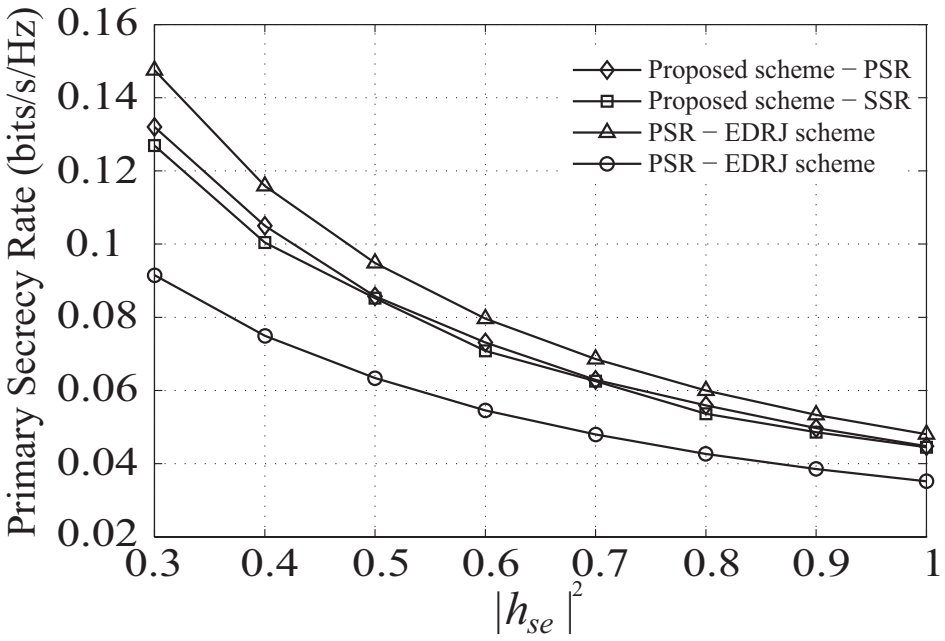

Figure 5.7: Secrecy rate: comparison with a friendly jammer without interference at the approach to the legitimate receiver

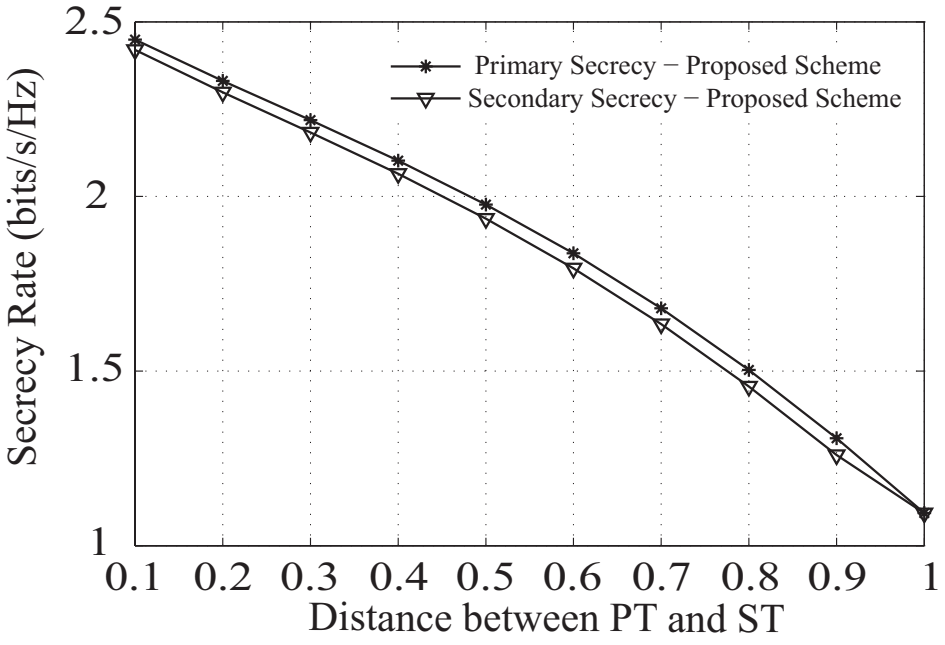

Figure 5.8: Secrecy rate versus distance between the PT and ST

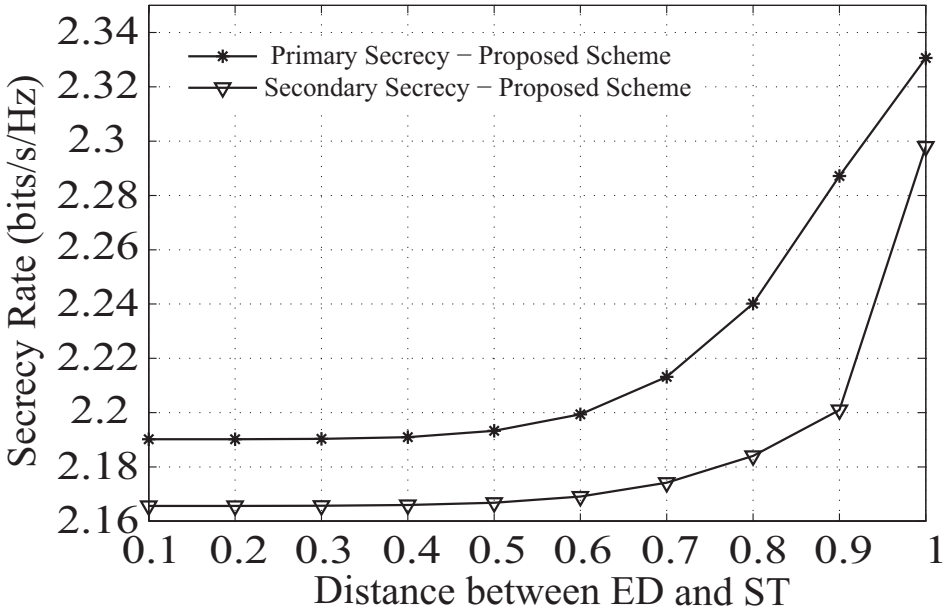

Figure 5.9: Secrecy rate versus distance between the ED and ST

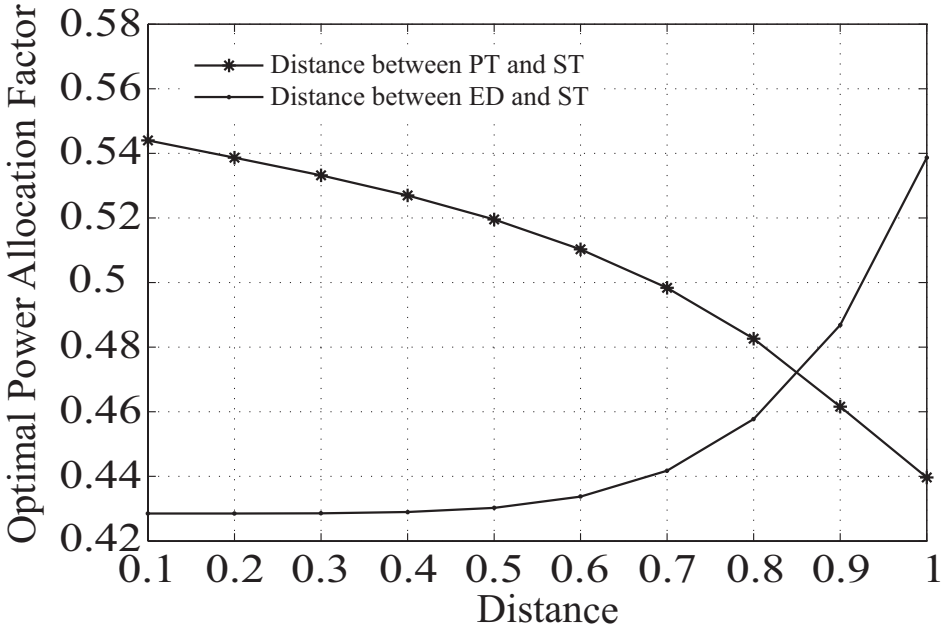

Figure 5.10: ϵ^* versus distance

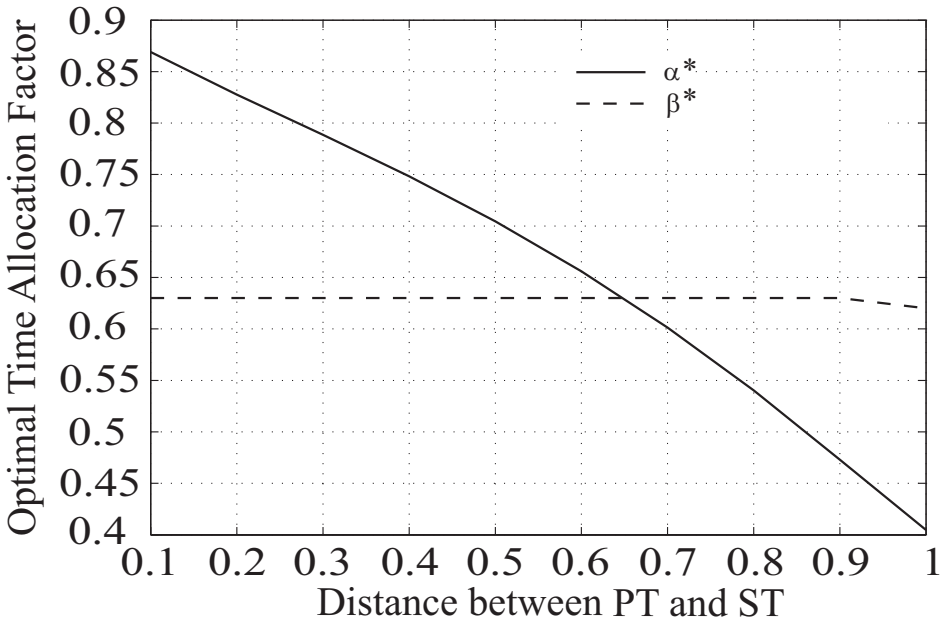

Figure 5.11: α^* and β^* versus distance between the PT and ST

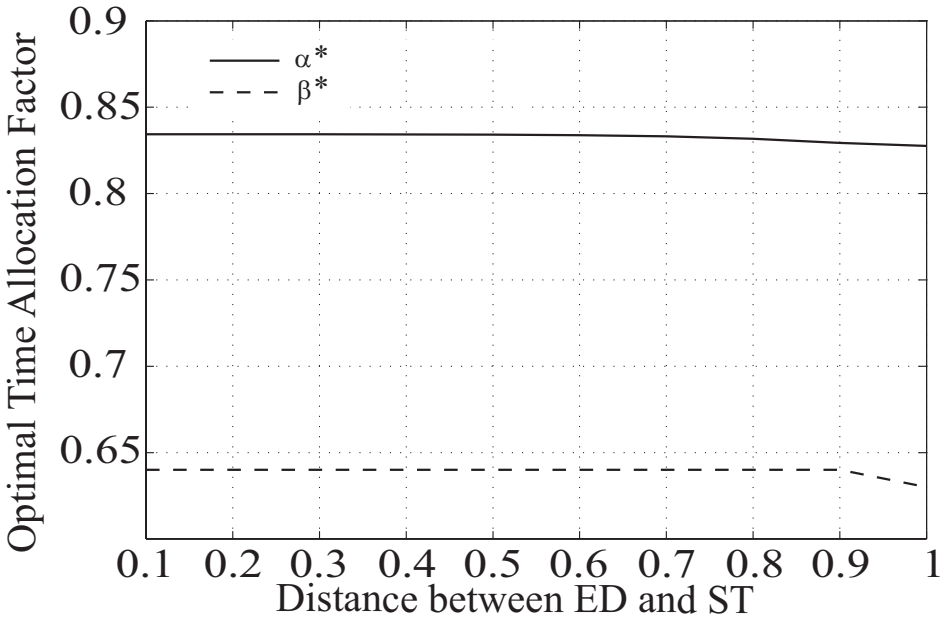

Figure 5.12: α^* and β^* versus distance between the ED and ST

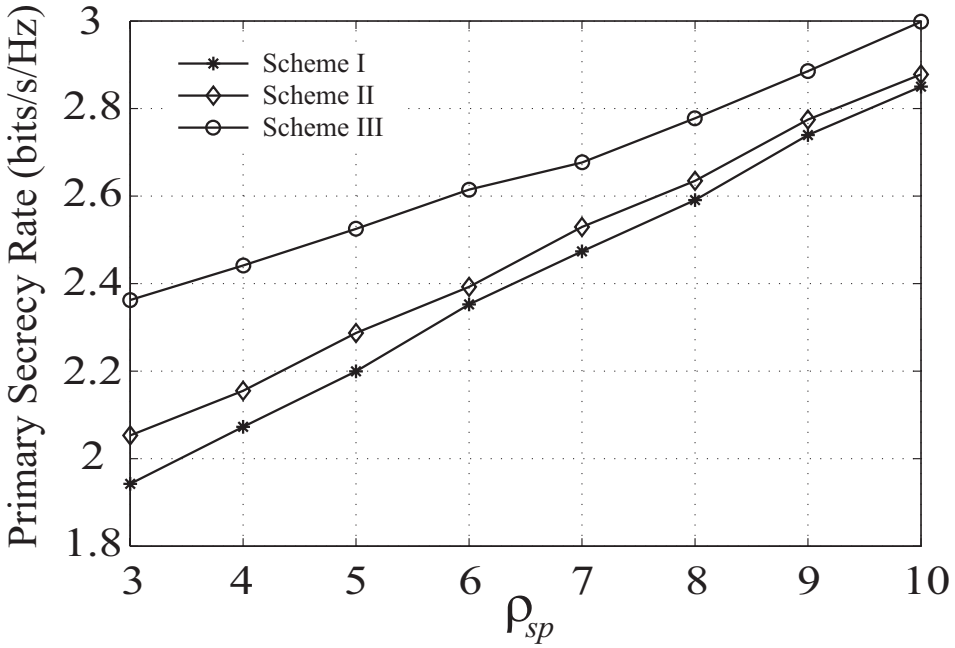

Figure 5.13: Primary secrecy rate versus ρ_{sp}

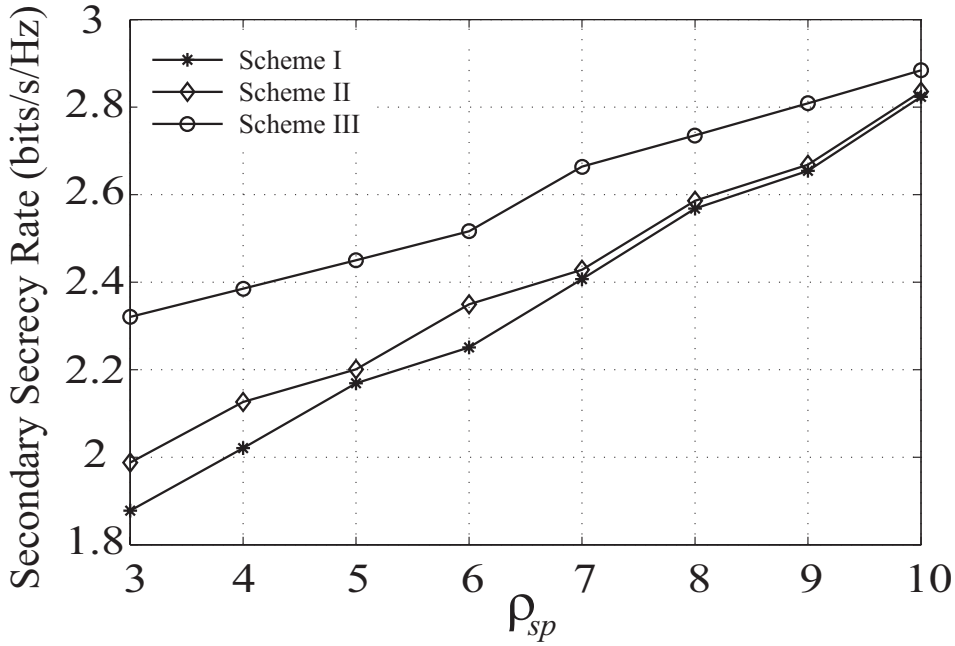

Figure 5.14: Secondary secrecy rate versus ρ_{sp}

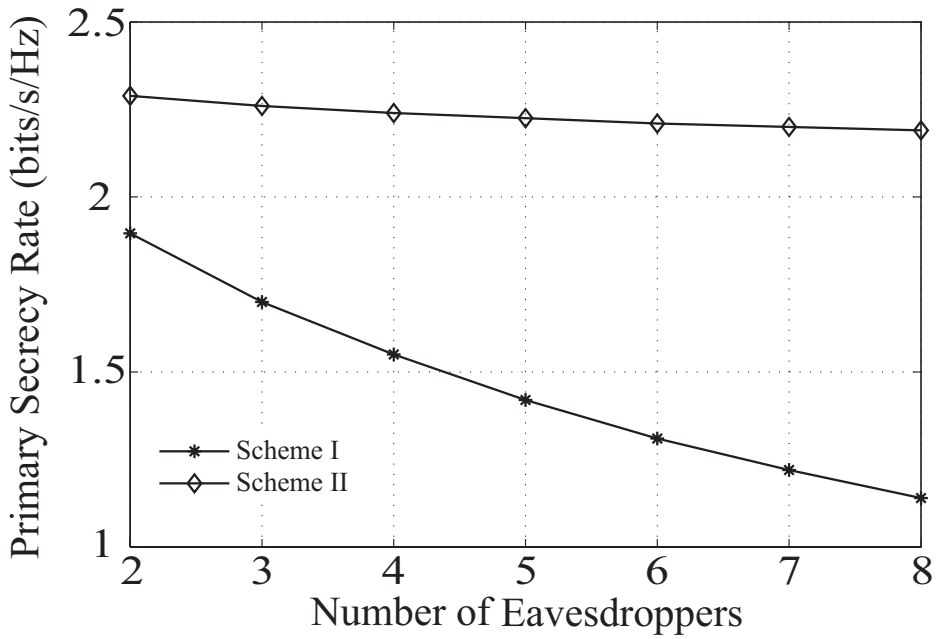

Figure 5.15: Primary secrecy rate versus the number of eavesdroppers

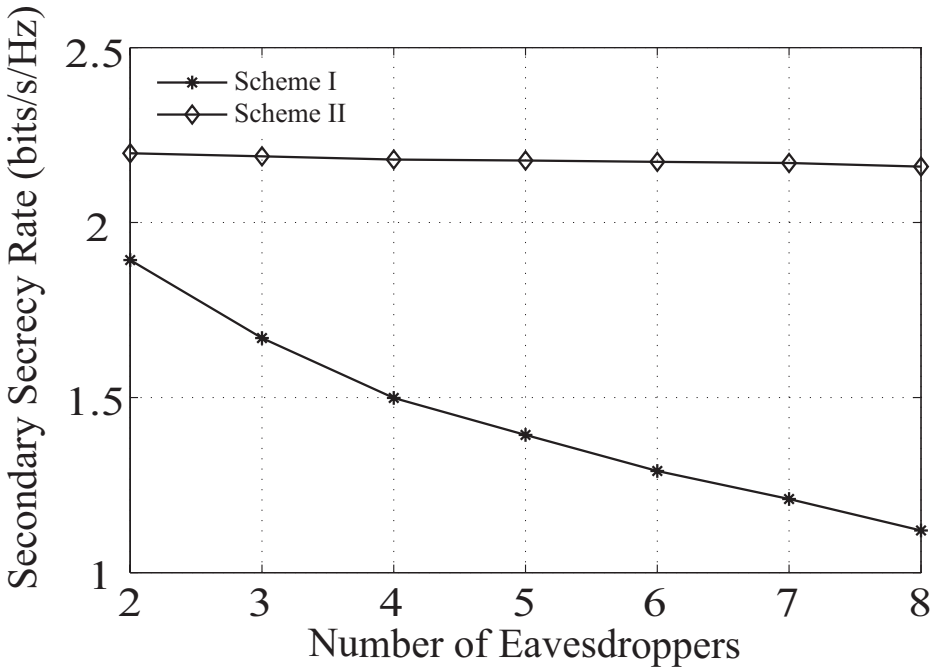

Figure 5.16: Secondary secrecy rate versus the number of eavesdroppers

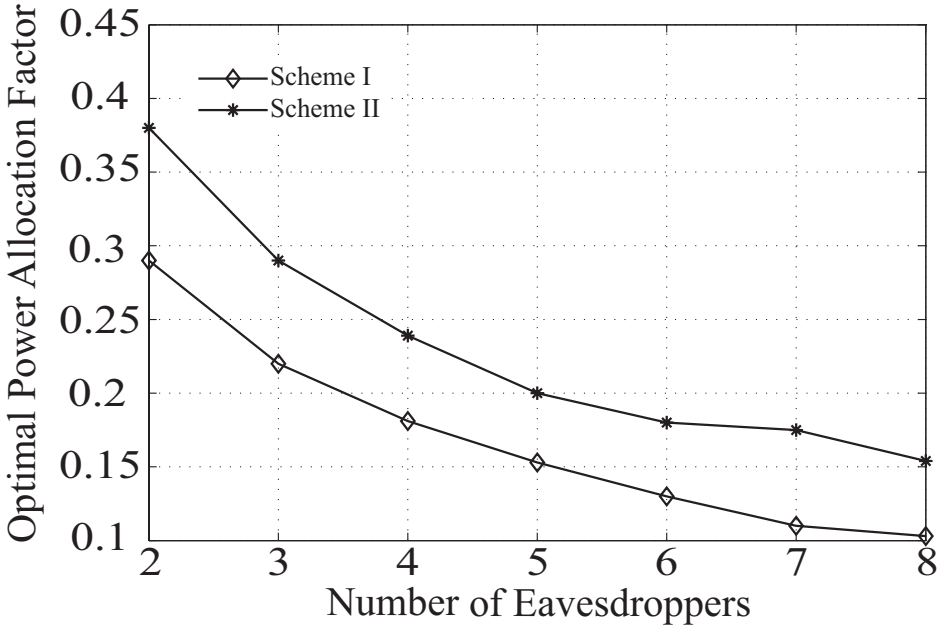

Figure 5.17: ϵ^* versus the number of eavesdroppers

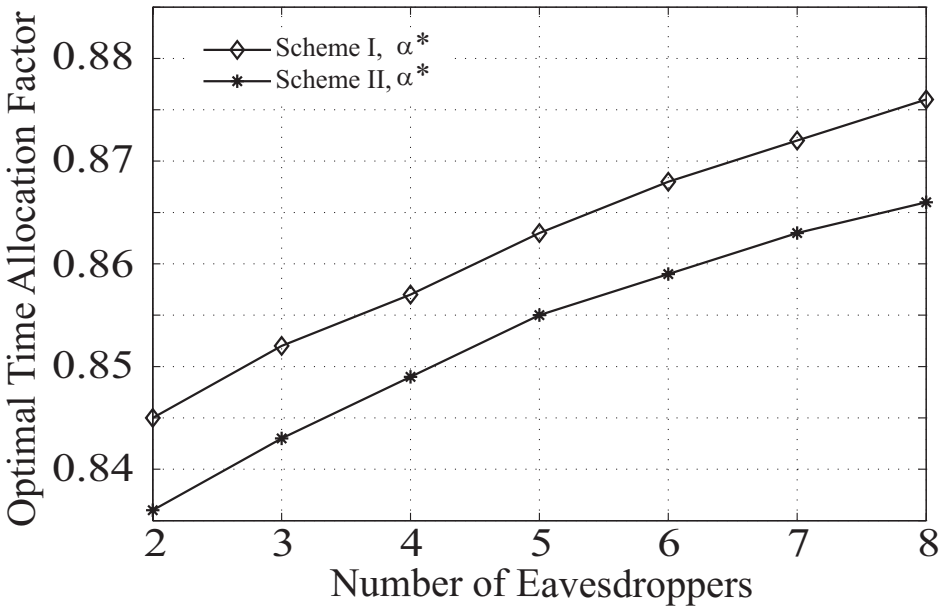

Figure 5.18: α^* versus the number of eavesdroppers

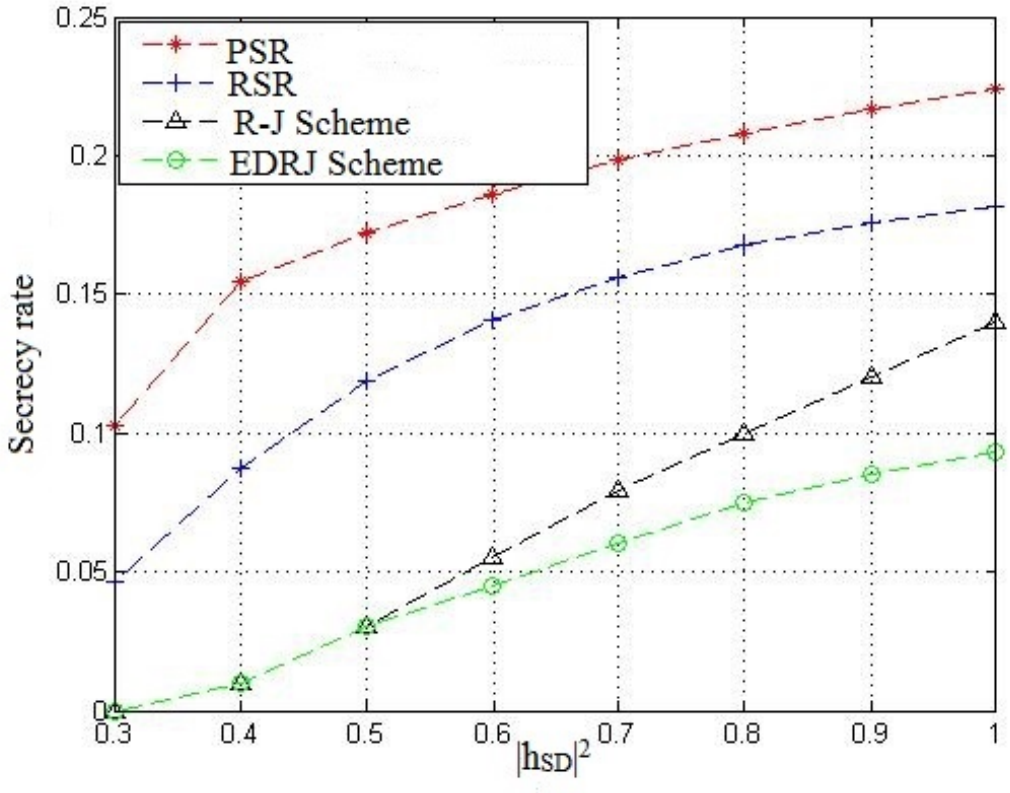

Figure 5.19: Comparison for the primary secrecy rate

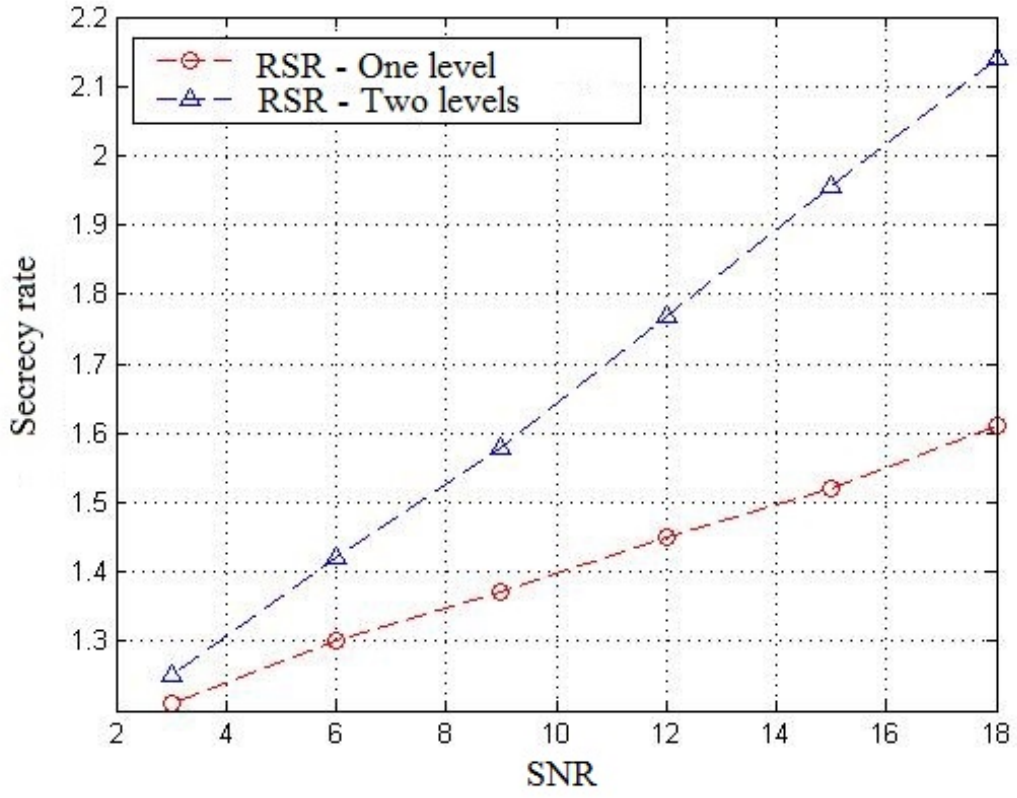

Figure 5.20: Comparison of the secrecy rate versus the SNR

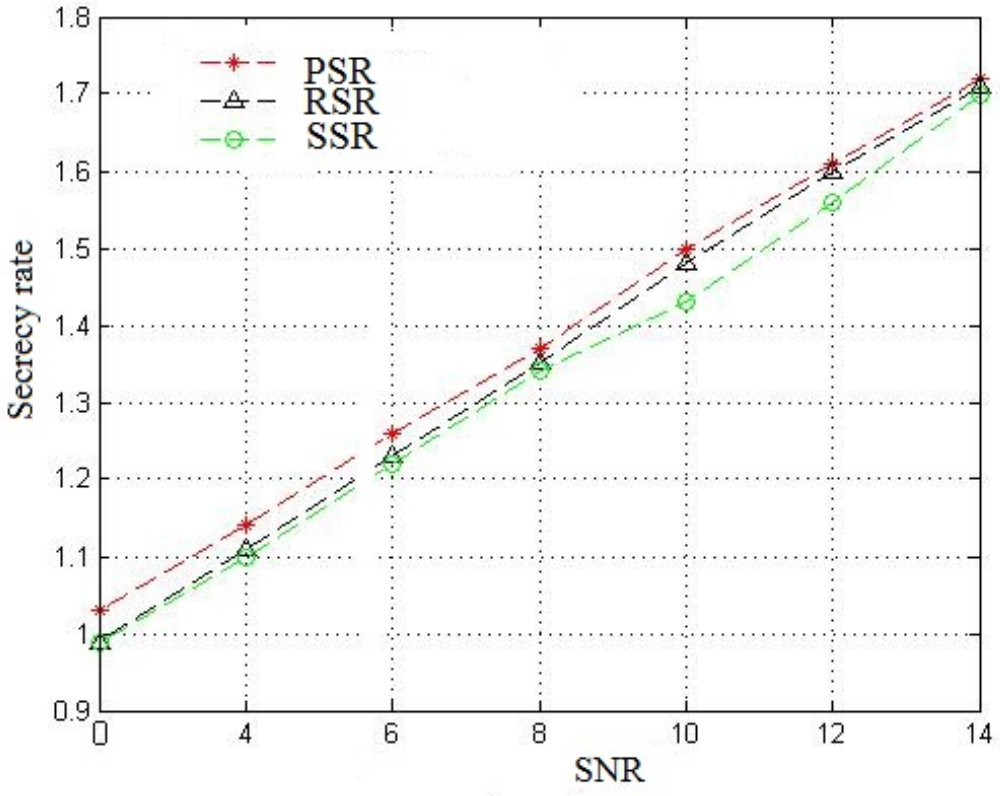

Figure 5.21: Secrecy rate versus the SNR

Chapter 6

Physical layer security of cognitive radio systems via distributive matching theory

In this chapter, cooperative spectrum sharing is considered in a cognitive radio network consisting of multiple primary and multiple secondary users. A particular focus is physical-layer security in cognitive radio networks, wherein multiple secondary nodes assist multiple primary nodes in combating unwanted eavesdropping from a malicious eavesdroppers. Two scenarios are considered: a single eavesdropper and multiple eavesdroppers. In Scenario I, the secondary users act as a relay and jammer, whereas the secondary users act as a jammer only in Scenario II. Multiple eavesdroppers are also considered, and are distributed according to a homogenous Poison Point Process (PPP). The primary and secondary secrecy rates are studied to find the solution of the developed matching game that yields a stable matching between the sets of the primary and secondary users. Closed forms for the outage probability and mean secrecy rate for both the primary and secondary transmissions are derived. Furthermore, the saleability and convergence of the matching theory are proved. Both the analytical and numerical results show that the proposed matching model is a promising approach under which the utility

functions of both primary and secondary users are maximised.

6.1 Introduction

A utility-based matching framework is proposed that motivates multiple primary nodes and multiple secondary nodes to cooperate with each other such that the sum-secrecy rate over all source nodes is maximised. Within the money transfer framework, primary nodes provide monetary compensation to motivate secondary nodes to allocate secondary power to relay the primary information signal and interfere with the eavesdropper. This will be achieved by utilising matching theory and auction theory, which provide a convenient framework for algorithm development and performance analysis. The main contributions of this study are summarised as follows:

1. To our knowledge, this study provides a novel framework that can address the general matching scenario to enhance security for both primary and secondary transmissions.

2. *Scenario I – single eavesdropper:* Matching theory and auction theory are applied to the allocated secondary power to relay the primary message and create interference with the eavesdropper. Simulation results show that the proposed scheme provides a significant increase in the primary secrecy rate (PSR) at the expense of a slight reduction in the secondary secrecy rate (SSR) in comparison with the corresponding central algorithm.

3. *Scenario I – multiple eavesdroppers:* Matching theory and auction theory are applied to the allocated secondary power to create interference with the eavesdroppers. Again, simulation results show that the proposed scheme provides a significant increase in the primary secrecy rate (PSR) at the expense of a slight reduction of the secondary secrecy rate (SSR) in comparison to the corresponding central algorithm.

4. *Scenario II – multiple eavesdroppers:* To highlight the impact of multiple eavesdroppers on the PSR and SSR, the proposed CR systems are analysed under the malicious attempt of multiple non-colluding eavesdroppers that are distributed according to a homogeneous Poisson point process (PPP) distribution around primary and secondary transmitters. It is shown that the mean secrecy rate achieved for CR systems under the non-colluding eavesdroppers is significantly higher than that under the traditional central algorithm.

The remainder of this chapter is organised as follows. In Section II, the system model and achievable secrecy rates for Scenario I are defined. In Section III, the optimisation problems are presented for the given scenarios and their matching game-theoretic approaches. Section IV presents the proposed algorithm to solve optimisation problems, and Section VI shows the convergence of PSMA. Section VII indicates the system model for the CR in Scenario II and the problem formulation for Scenario II. These scenarios are then compared via numerical simulations in Section VIII, and Section IX presents and discusses the numerical results. Finally, Section X concludes the chapter.

6.2 System model

In this section, a CRN is considered, illustrated in Figure 6.1, consisting of N pairs of a primary transmitter node, PT_i, and its corresponding receiver node, PR_i (where $i = 1, 2, \cdots, N$), M pairs of a secondary transmitter node ST_j and its corresponding secondary receiver node, SR_j (where $j = 1, 2, \cdots, M$), and a malicious eavesdropper (ED). It is assumed that the primary pairs, secondary receivers, and ED have single antennae, while the secondary transmitters have K transmit antennas each. The ST_js can play the role of a relay and the relay selection will be carried out based on the matching game.

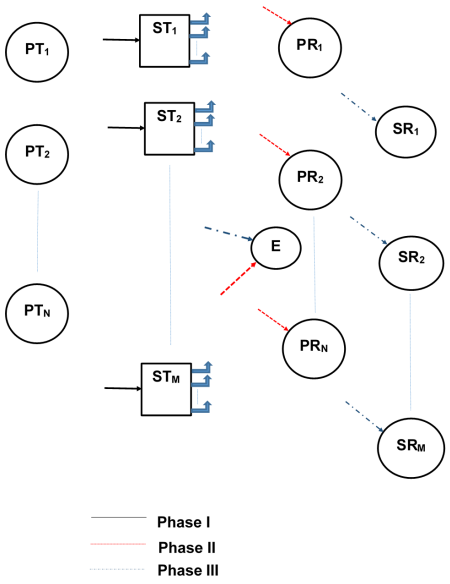

Figure 6.1: The considered scenario

In general, the secrecy rate R_{sec} is defined as:

$$R_{sec} = (R_D - R_E)^+, \tag{6.1}$$

where R_D and R_E are the information rates at the destination and eavesdropper, respectively; and $(x)^+ = \max(0, x)$ refers to the positivity value of the secrecy rate. For convenience, the $(\cdot)^+$ sign is omitted from subsequent calculations.

6.2.1 Mathematical models

The system has three phases as follows:

1) Phase 1: The PT_is decide to cooperate by using a fraction $(1 - T)$ of the whole time slot for transmission from the primary nodes to the preferred secondary node, ST_j (where $0 < T < 1$). The remaining fraction will be used in Phases 2 and 3. It is assumed that transmission from the PT_is is invisible at the ED. In this first phase, each ST_j can be used as a relay and the received signal at ST_j is

$$x_{i,j}^{(ST)} = \sqrt{P_p} h_{i,j}^{(ps)} s_i + n_j^{(ST)}, \tag{6.2}$$

where s_i is the primary message signal from the PT_i with transmission power P_p,

$n_j^{(ST)} \sim \mathcal{N}(0, \sigma^2)$ is the noise at ST_j, and $h_{i,j}^{(ps)} \sim \mathcal{N}(0, \sigma_h^2)$ is the channel coefficient between the PT_i and ST_j. For notational convenience, let us define

$$\rho_{i,j}^{(ps)} = \frac{P_p \left(h_{i,j}^{(ps)}\right)^2}{\sigma^2}.$$

Then, the information rate at the ST_j, denoted by $R_{i,j}^{(ps)}$, is given by

$$R_{i,j}^{(ps)} = \frac{(1-T)\log_2(1+\rho_{i,j}^{(ps)})}{2}. \tag{6.3}$$

2) Phase 2: The ST_j, having multiple transmit antennas, forwards the secure primary message to the PR_i within the fraction $\alpha(1-T)$ (where $0 < \alpha < 1$) of the considered time slot. In this phase, for security reasons, the ST_j also transmits the artificial noise z_j in addition to the re-encoded primary signal $\hat{s}_i$ using power vectors $\mathbf{v}_j$ and $\mathbf{u}_j$, respectively. The received signal at the ith primary receiver PR_i is

$$x_{j,i}^{(PR)} = \sqrt{P_s}\mathbf{h}_{j,i}^{(sp)}\mathbf{u}_j\hat{s}_i + \sqrt{P_s}\mathbf{h}_{j,i}^{(sp)}\mathbf{v}_j z_j + n_i^{(PR)}, \tag{6.4}$$

where $\mathbf{h}_{j,i}^{(sp)} \sim \mathcal{N}(\mathbf{0}_K, d_{j,i}^{-\beta}\mathbf{I}_K)$ is the channel vector (of length K due to K multiple transmit antennas at ST_j) between ST_j and PR_i, β is the pass loss exponent, and $d_{j,i}$ is the distance between ST_j and PR_i. The received signal at the ED in Phase 2 is

$$x_{ED,j}^{(2)} = \sqrt{P_s}\mathbf{h}_j^{(se)}\mathbf{u}_j\hat{s}_i + \sqrt{P_s}\mathbf{h}_j^{(se)}\mathbf{v}_j z_j + n_j^{(ED)}, \tag{6.5}$$

where $\mathbf{h}_j^{(se)} \sim \mathcal{N}(\mathbf{0}_K, d_{j,E}^{-\beta}\mathbf{I}_K)$ is the channel vector between the ST_j and the ED, and the distance between them is $d_{j,E}$. The information rate at PR_i is then

$$R_{PR_i} = \frac{1}{2}T\alpha\log_2\left(1 + \frac{P_s\left|\left(\mathbf{h}_{j,i}^{(sp)}\right)^\dagger \mathbf{U}_j\mathbf{h}_{j,i}^{(sp)}\right|}{\sigma^2 + P_s\left|\left(\mathbf{h}_{j,i}^{(sp)}\right)^\dagger \mathbf{V}_j\mathbf{h}_{j,i}^{(sp)}\right|}\right), \tag{6.6}$$

where $\mathbf{U}_j = \mathbf{u}_j\mathbf{u}_j^\dagger$ and $\mathbf{V}_j = \mathbf{v}_j\mathbf{v}_j^\dagger$. At the same time, the information rate at the ED in Phase 2 is

$$R_{ED}^{(2)} = \frac{1}{2}T\alpha\log_2\left(1 + \frac{P_s\left|\left(\mathbf{h}_j^{(se)}\right)^\dagger \mathbf{U}_j\mathbf{h}_j^{(se)}\right|}{\sigma^2 + P_s\left|\left(\mathbf{h}_j^{(se)}\right)^\dagger \mathbf{V}_j\mathbf{h}_j^{(se)}\right|}\right). \tag{6.7}$$

According to Equation (6.1), the achievable primary secrecy rate (PSR), denoted by $R_{j,i}^{(PSR)}$, can be obtained as follows:

$$\begin{aligned} R_{j,i}^{(PSR)} &= R_{PR_i} - R_{ED}^{(2)} \\ &= \frac{1}{2}T\alpha \left[\log_2 \left(1 + \frac{P_s \left| \left(\mathbf{h}_{j,i}^{(sp)} \right)^{\dagger} \mathbf{U}_j \mathbf{h}_{j,i}^{(sp)} \right|}{\sigma^2 + P_s \left| \left(\mathbf{h}_{j,i}^{(sp)} \right)^{\dagger} \mathbf{V}_j \mathbf{h}_{j,i}^{(sp)} \right|} \right) \right. \\ &- \left. \log_2 \left(1 + \frac{P_s \left| \left(\mathbf{h}_{j}^{(se)} \right)^{\dagger} \mathbf{U}_j \mathbf{h}_{j}^{(se)} \right|}{\sigma^2 + P_s \left| \left(\mathbf{h}_{j}^{(se)} \right)^{\dagger} \mathbf{V}_j \mathbf{h}_{j}^{(se)} \right|} \right) \right]. \end{aligned} \tag{6.8}$$

3) Phase 3: The ST_j can now send its own secure secondary message, s_j, to the SR_j within the remaining faction $T(1-\alpha)$ of the considered time slot, using the power allocation vector $\mathbf{u}'_j$. Again, it is assumed that the same codeword for artificial noise (with power allocation vector $\mathbf{v}'_j$) and the same power allocation strategy are used for this secondary transmission. The received signal at the SR_j is

$$x_j^{(SR)} = \sqrt{P_s}\mathbf{h}_j^{(ss)}\mathbf{u}'s_j + \sqrt{P_s}\mathbf{h}_j^{(ss)}\mathbf{v}'_j z_j + n_j^{(SR)}, \tag{6.9}$$

where $\mathbf{h}_j^{(ss)} \sim \mathcal{N}(\mathbf{0}_K, d_{j,j}^{-\beta}\mathbf{I}_K)$ is the channel vector of length K between ST_j and SR_j. The received signal at the ED in Phase 3 is

$$x_{ED,j}^{(3)} = \sqrt{P_s}\mathbf{h}_j^{(se)}\mathbf{u}'_j s_j + \sqrt{P_s}\mathbf{h}_j^{(se)}\mathbf{v}'_j z_j + n_j^{(ED)}. \tag{6.10}$$

The information rate at the SR_j is obtained by

$$R_{SR_j} = \frac{1}{2}T(1-\alpha)\log_2 \left(1 + \frac{P_s \left| \left(\mathbf{h}_j^{(ss)} \right)^{\dagger} \mathbf{U}'_j \mathbf{h}_j^{(ss)} \right|}{\sigma^2 + P_s \left| \left(\mathbf{h}_j^{(ss)} \right)^{\dagger} \mathbf{V}'_j \mathbf{h}_j^{(ss)} \right|} \right), \tag{6.11}$$

where $\mathbf{U}'_j = \mathbf{u}'_j \left(\mathbf{u}'_j\right)^{\dagger}$ and $\mathbf{V}'_j = \mathbf{v}'_j \left(\mathbf{v}'_j\right)^{\dagger}$. Also, the information rate at the ED in this phase (Phase 3) is given by

$$R_{ED}^{(3)} = \frac{1}{2}T(1-\alpha)\log_2 \left(1 + \frac{P_s \left| \left(\mathbf{h}_j^{(se)} \right)^{\dagger} \mathbf{U}'_j \mathbf{h}_j^{(se)} \right|}{\sigma^2 + P_s \left| \left(\mathbf{h}_j^{(se)} \right)^{\dagger} \mathbf{V}'_j \mathbf{h}_j^{(se)} \right|} \right). \tag{6.12}$$

Similarly, the secondary secrecy rate (SSR), denoted by $R_j^{(SSR)}$, can be obtained as follows:

$$\begin{aligned} R_j^{(SSR)} &= R_{SR_j} - R_{ED}^{(3)} = \frac{1}{2}T(1-\alpha) \\ &\quad \times \left[\log_2 \left(1 + \frac{P_s \left| \left(\mathbf{h}_j^{(ss)} \right)^\dagger \mathbf{U}_j' \mathbf{h}_j^{(ss)} \right|}{\sigma^2 + P_s \left| \left(\mathbf{h}_j^{(ss)} \right)^\dagger \mathbf{V}_j' \mathbf{h}_j^{(ss)} \right|} \right) \right. \\ &\quad \left. - \log_2 \left(1 + \frac{P_s \left| \left(\mathbf{h}_j^{(se)} \right)^\dagger \mathbf{U}_j' \mathbf{h}_j^{(se)} \right|}{\sigma^2 + P_s \left| \left(\mathbf{h}_j^{(se)} \right)^\dagger \mathbf{V}_j' \mathbf{h}_j^{(se)} \right|} \right) \right]. \end{aligned} \tag{6.13}$$

6.2.2 Utility function and problem formulation for enhancing security

It is assumed that the ST_js and PR_is have global instantaneous CSI information and that ST_j has the knowledge of the CSI to the ED and the CSI between PR_i and SR_j. The utility function of the primary transmission can be selected to be increasing with α and decreasing with the eavesdropper's information rate. The primary utility, denoted by $U_{P_{j,i}}$, can be written as

$$U_{P_{j,i}} = R_{PR_i} - R_{ED}^{(2)} + c_p P_s, \tag{6.14}$$

where c_p is a pricing constant. Moreover, the utility of the secondary transmission, denoted by $U_{S_{j,j}}$, can be written as

$$U_{S_{j,j}} = R_{SR_j} - R_{ED}^{(3)} - c_p P_s. \tag{6.15}$$

Given the channel knowledge, its power weight vector can be designed to maximize interference to the ED while minimising the interference to both PR_i and SR_j. The solution of the weight vector for the secondary transmission is given by

$$\begin{aligned} \mathbf{v}_j'^* = \arg \max_{0<\alpha<1} & \left| \left(\mathbf{h}_j^{(se)} \right)^\dagger \mathbf{V}_j' \mathbf{h}_j^{(se)} \right| \\ \text{s.t.} \quad & \left| \left(\mathbf{h}_j^{(ss)} \right)^\dagger \mathbf{V}_j' \mathbf{h}_j^{(ss)} \right| = 0, \\ & |\mathbf{v}_j' \left(\mathbf{v}_j' \right)^\dagger| = 1. \end{aligned} \tag{6.16}$$

Using projection matrix theory to provide the solution of the optimisation problem in Equation (6.16), $\left|\mathbf{v}_j'^*\right|$ can be achieved as follows:

$$|\mathbf{v}_j'^*| = \frac{(\mathbf{I} - \mathbf{h}_j^{(ss)}(\mathbf{h}_j^{(ss)}\mathbf{h}_j^{(ss)\dagger})^{-1}\mathbf{h}_j^{(ss)\dagger})\mathbf{h}^{(se)}}{\left|(\mathbf{I} - \mathbf{h}_j^{(ss)}(\mathbf{h}_j^{(ss}\mathbf{h}_j^{(ss)\dagger})^{-1}\mathbf{h}_j^{(ss)\dagger})\mathbf{h}^{(se)}\right|}. \tag{6.17}$$

Similarly, using the above method, the optimal solution of $\mathbf{v}_j$ in the primary transmission can be obtained by solving the following problem:

$$\begin{aligned} \mathbf{v}_j^* = &\arg \max_{0<\alpha<1} \left|\left(\mathbf{h}_j^{(se)}\right)^\dagger \mathbf{V}_j \mathbf{h}_j^{(se)}\right| \\ \text{s.t.} \quad &\left|\left(\mathbf{h}_{j,i}^{(sp)}\right)^\dagger \mathbf{V}_j \mathbf{h}_{j,i}^{(sp)}\right| = 0, \\ &|\mathbf{v_j}\mathbf{v_j^\dagger}| = 1. \end{aligned} \tag{6.18}$$

The solution is then given by

$$|\mathbf{v}_j^*| = \frac{(\mathbf{I} - \mathbf{h}_{j,i}^{(sp)}(\mathbf{h}_{j,i}^{(sp)}\mathbf{h}_{j,i}^{(sp)\dagger})^{-1}\mathbf{h}_{j,i}^{(sp)\dagger})\mathbf{h}^{(se)}}{\left|(\mathbf{I} - \mathbf{h}_{j,i}^{(sp)}(\mathbf{h}_{j,i}^{(sp)}\mathbf{h}_{j,i}^{(sp)\dagger})^{-1}\mathbf{h}_{j,i}^{(sp)\dagger})\mathbf{h}^{(se)}\right|}. \tag{6.19}$$

6.3 Matching theory and formulation of the optimisation problem

In this section, PT_i will be paired with ST_j using matching theory. It is convenient to first introduce some notation in matching theory.

Definition 1: A matching function is defined:

$$\begin{aligned} \psi : \{p_i : i \in PT \cup \{0\}\} \cup \{s_i : i \in ST \cup \{0\}\} \\ \rightarrow \{p_i : i \in PT \cup \{0\}\} \cup \{s_i : i \in ST \cup \{0\}\} \\ \times \{\mathbb{R}^+ \cup \{0\}\} \end{aligned} \tag{6.20}$$

such that for all $p_i \in PT$ and $s_j \in ST$:

1. $\psi(p_i) = (s_0, \alpha_{i,0}) \Rightarrow \alpha_{i,0} = 0$ and $P_s = 0$.

2. $\psi(s_j) = (p_0, \alpha_{0,j}) \Rightarrow \alpha_{0,j} = 0$ and $c_p = 0$.

3. $\psi(p_i) = (s_j, \alpha_{i,j}) \Leftrightarrow \psi(s_j) = (p_i, \alpha_{i,j})$.

A dummy primary transmitter node (p_0) and a dummy secondary transmitter node (s_0) can be considered, which are convenient for notational purposes. To see this, in Step 1 of Definition 1, a primary node is considered that is "not matched"; that is, no secondary node is cooperating with this primary node, which is equivalent to $\alpha_{i,0} = 0$ and secondary power. In Step 2 of Definition 1, if a secondary node is "not matched," i.e., it does not provide relay services for any primary node, then it follows that the utility for this secondary node is zero. Finally, it is implied that p_i is matched to s_j with $\alpha_{i,j}$ and then s_j is matched to p_i with $\alpha_{i,j}$.

According to the matching definition, the following objective problem can be considered for the total secrecy rate (TSR_1) by summing the primary and secondary utilities:

$$TSR_1 = \sum_{i=1}^{N} \sum_{j=1}^{M} m_{i,j}(U_{P_{j,i}} + U_{S_{j,j}}), \tag{6.21}$$

where $m_{i,j} = 1$ if p_i and s_j are matched and $m_{i,j} = 0$ otherwise. It can be concluded that

$$TSR_1 = \sum_{i=1}^{N} \sum_{j=1}^{M} m_{i,j}(R_{j,i}^{(PSR)} + R_j^{(SSR)}). \tag{6.22}$$

The objective of our problem is now to find the matching matrix that maximises the total secrecy rate of the cognitive network. Therefore, the following is considered:

$$M_1 = \arg \max_{m_{i,j}<1, i\in P, j\in S} \sum_{i=1}^{N} \sum_{j=1}^{M} m_{i,j}(R_{j,i}^{(PSR)} + R_j^{(SSR)}). \tag{6.23}$$

A distributive algorithm is proposed to solve this problem, as detailed in the next section.

6.4 Proposed distributive algorithm

In order to solve the problem given by Equation (6.23), the primary-secondary matching algorithm (PSMA) is now proposed, which is inspired by the deferred

acceptance algorithm. A new function is first defined:

$$\theta_{i,j} = \begin{cases} 1, & \text{if PT}_j \text{ is in the highest priority position} \\ & \qquad \text{of the secondary user list, and} \\ 0, & \text{otherwise.} \end{cases} \tag{6.24}$$

Details of the algorithm are as follows:

1. *Step 1: Initialisation*

   (a) Each PT_i broadcasts its α, where $\alpha > \alpha_{min}$, to all STs and constructs its preference list, *PTList*. Also, the unmatched list of primary users, *UML*, is constructed.

   (b) Each ST_j constructs its preference list, *STList*, according to the announced α.

2. *Step 2: Main implementation*

   (a) PT_i offers $\alpha_{i,j}$ to the first SU_j in its preference list.

   (b) If ST_j is not matched and PT_i is in its preference list, then the matching index $m_{i,j} = 1$ and PT_i is removed from the *UML*.

   (c) Else if ST_j is already matched to the current primary user, PT_{curr}, but PT_i has higher priority than PT_{curr} in the preference list of ST_j, then ST_j will match to PT_i with $m_{i,j} = 1$ and put PT_{curr} in the *UML*.

   (d) Else if

   $$\sum_{j=1}^{M} \theta_{i,j} > 1,$$

   meaning that PT_i is located at the highest priority level in at least two secondary users' preference lists, then

   $$\alpha^{(it+1)} = \alpha^{(it)} + \delta,$$

   where δ is the step size and (it) is an iteration index. Then, update PT_i and return to the first part of Step 2.

(e) If PT_i is not in the preference list of ST_j and ST_j is still not matched with $\alpha^(it) > \alpha_{min}$, then let $\alpha^{(it+1)} = \alpha^{(it)} - \delta$ with $\alpha^(it) > \alpha_{min}$ and update its preference list according to the new value of α.

3. *Step 3: if UML $\neq \phi$, return to Step 2*

Definition 2: A matching is defined as stable if it is not blocked by any individual or any pair. It should be noted that, in order to achieve a stable matching, the number of primary node pairs does not have to be equal to the number of relays (i.e., $M \neq N$).

Lemma 9. *The PSMA converges to a stable matching.*

Proof: Please see Appendix A. ■

Definition 3: The matching and the allocated time slot (α), which are produced by the PSMA, are said to be in competitive equilibrium if the following conditions are satisfied:

1. The matched relay S_j always receives a non-negative utility (i.e. $\alpha_{i,j} \geq \alpha_{min}$).

2. Each PT is matched with the relay that provides the highest positive primary utility as follows:

$$\arg\max_{s_j} U_{p_{j,i}}, if \psi(p_i) = (s_j, \alpha_{i,j}), \psi(s_j) = (p_i, \alpha_{i,j}).$$

3. If the P_i is not matched, then $\alpha_{i,j} = \alpha_{min}$.

Theorem 3. *The matching and the allocated time slot (α) produced by the PSMA are in competitive equilibrium for small values of δ.*

Proof: According to the conditions in Definition 3, the PSMA must satisfy the conditions in 1, 2, and 3. From Step 1-a of the PSMA, if each PT_i offers at least α_{min} to the relay ST_j, then the relay satisfies Condition 1. From Step 2-d of the PSMA, $\alpha^{(it+1)} \geq \alpha^{(it)}$, since the primary utility has an increasing function with α, and it follows that it has a higher value in the next iteration. From Step 2-e of the

PSMA, since PT continues to reduce its α offer if the PT is not matched and its $\alpha \geq \alpha_{min}$, it follows that the PT's α equals at least α_{min} if the PT is not matched. ■

6.5 Convergence of the PSMA

The convergence behaviour of the PSMA is presented in the following theorem.

Theorem 4. *The upper limit of iterations needed to converge for the PSMA is*

$$L = (\alpha^{max} - \alpha_{min})/\delta, \tag{6.25}$$

where $0 < \alpha^{max}, \alpha_{min}, \delta < 1$ and

$$\alpha^{max} = \max_{PT_i} \alpha_{max,i}.$$

Proof: According to Step 2-d of the PSMA, α is incremented by δ when the PT has offers from at least two STs wishing to relay the PT's signal. Therefore, the PT cannot obtain matching with an ST at $\alpha_{max} + \delta$. On the other hand, from Step 2-e of the PSMA, if α is decremented by δ because the PT remains unmatched, and its $\alpha > \alpha_{min}$, then the PT cannot also match with the ST at $\alpha_{min} - \delta$. Thus, it can be concluded that in the worst case, the PT will match after $(\alpha^{max} - \alpha_{min})/\delta$ iterations. ■

6.6 Extension to non-colluding eavesdroppers (Scenario II)

Scenario II, which has non-colluding eavesdroppers, is considered in order to highlight the effect of multiple eavesdroppers on the secrecy rates. In this scenario, the multiple eavesdroppers are distributed according to a PPP, and it is not possible to apply a projection matrix to design the weighting of precoding to maximise

interference at the eavesdropper. However, the precoding weight $|\mathbf{w}_J|$ can be selected to satisfy the following two conditions:

1. $\left|\left(\mathbf{h}_{j,i}^{(sp)}\right)^{\dagger}\mathbf{w}_j\right| = 0.$
2. $|\mathbf{w}_J\mathbf{w}_J{}^{\dagger}| = 1.$

To satisfy these conditions, it is necessary to send $|\mathbf{w}_J|$ in the null space of $\mathbf{h}_{j,i}^{(sp)}$. Then the information rate at PR can be written as

$$R_{i,i}^{(PP)} = \alpha \log_2(1 + \rho_{i,i}^{(pp)}), \tag{6.26}$$

where $\rho_i = \frac{P_p\left|h_{i,i}^{(pp)}\right|}{\sigma^2}$. As a worst case, it is assumed that each ED can cancel the interference from other primary users. In this case, the ED receives the useful signal embedded in the jamming signal and noise. The leakage rate at the l^{th} ED can be written as

$$R_{PE,l} = \alpha \log_2 \left(1 + \mathbb{E}_{l\in\phi_e} \frac{P_p h_l^{(PE)}}{\sigma^2 + P_s \left|\mathbf{h}_l^{(SE)^{\dagger}}\mathbf{w}_J\right|^2}\right). \tag{6.27}$$

According to Equation (6.1), the achievable primary secrecy rate (PPR), denoted by R_i, can be obtained as follows:

$$\begin{aligned} R_i &= R_{i,i}^{(PP)} - R^{(PE)} \\ &= \alpha \left[\log_2(1 + \rho_{i,i}^{(pp)}) - \log_2(1+ \right. \\ &\qquad \left. \mathbb{E}_{l\in\phi_e} \frac{P_p h_l^{(PE)}}{\sigma^2 + P_s \left|\mathbf{h}_l^{(SE)^{\dagger}}\mathbf{w}_J\right|^2})\right]. \end{aligned} \tag{6.28}$$

2) Phase 2: The ST_j transmits the secondary message to SR_j at time slot $(1-\alpha)$ in the presence of non-colluding eavesdroppers. The SR_j extracts only the information signal because the precoding weighting $\mathbf{v}_j'$ can send only in the null space of $\rho^{(ss)}$, which in turn is because of the PPP distribution of multiple eavesdroppers. The information rate at the SR_j is

$$R_{j,j}^{(SS)} = (1-\alpha)\log_2(1 + \rho_{j,j}^{(ss)}), \tag{6.29}$$

while the leakage rate at the lth eavesdropper can be written as

$$R_{ED}^{(2)} = (1-\alpha)\log_2\left(1+\mathbb{E}_{l\in\phi_e}\frac{P_s\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger\mathbf{u}_j'\right|^2}{\sigma^2+P_s\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger\mathbf{v}_j'\right|^2}\right). \tag{6.30}$$

Furthermore, the secondary secrecy rate (SSR), denoted by R_j, can be obtained as follows:

$$\begin{aligned} R_j &= R_{SR_j} - R_{ED}^{(2)} = (1-\alpha) \\ &\times\left[\log_2\left(1+\frac{P_s\left|\left(\mathbf{h}_l^{(ss)}\right)^\dagger\mathbf{u}_j'\right|^2}{\sigma^2+P_s\left|\left(\mathbf{h}_l^{(ss)}\right)^\dagger\mathbf{v}_j'\right|^2}\right)\right. \\ &- \left.\log_2\left(1+\mathbb{E}_{l\in\phi_e}\frac{P_s\left|\left(\mathbf{h}_l^{(se)}\right)^\dagger\mathbf{u}_j'\right|^2}{\sigma^2+P_s\left|\left(\mathbf{h}_l^{(se)}\right)^\dagger\mathbf{v}_j'\right|^2}\right)\right]. \end{aligned} \tag{6.31}$$

6.7 Outage probability and mean secrecy rate in Scenario II

This section derives the outage probability and the mean secrecy rate over the location of the external non-colluding eavesdroppers. In non-colluding eavesdroppers, the SINR at the nearest ED in Phase I can be given by

$$\gamma_{E,i} = \max_{l\phi_e}\frac{P_p h_l^{(PE)}}{\sigma^2+P_s\left|\mathbf{h}_l^{(SE)\dagger}\mathbf{w}_J\right|^2}, \tag{6.32}$$

and the SINR at ED in Phase II can be written as

$$\gamma_{E,j} = \max_{l\in\phi_e}\frac{P_s\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger\mathbf{u}_j'\right|^2}{\sigma^2+P_s\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger\mathbf{v}_j'\right|^2}. \tag{6.33}$$

6.7.1 Outage probability of primary and secondary transmissions

Lemma 10. *The secrecy outage probability at the primary receiver, which is caused by colluding eavesdroppers, can be written as the following, with a path loss coefficient of 4:*

$$\begin{aligned} P_{(o_E,i)} &= \frac{\pi^{\frac{3}{2}}\lambda_e}{2}\sqrt{\frac{P_p}{N\rho_i\sigma^2}} \\ &\quad \exp\left(\frac{\pi^3\lambda_e^2 P_s \exp(1/N^{-8})}{4\sigma^2}\right) \\ &\quad erfc\left[\frac{\pi^{\frac{3}{2}}\lambda_e\sqrt{P_s}\exp(1/N^{-4})}{2\sqrt{\sigma^2}}\right]. \end{aligned} \tag{6.34}$$

Proof: Please see Appendix B. ■

Lemma 11. *When considering the special case of the path loss coefficient being equal to 4, the secrecy outage probability at the jth SR, which is caused by the nearest eavesdropper, can be written as:*

$$\begin{aligned} P_{o_E,k} &= \frac{\pi^{3/2}\lambda_e\sqrt{P_s(1-\rho_j)}}{2\sqrt{N\sigma^2\rho_j}} \\ &\quad \exp\left[\frac{(\pi\lambda_e)^2 P_s(1-\rho_j)}{4N\sigma^2\rho_j}\right] \\ &\quad erfc\left(\frac{\pi\lambda_e\sqrt{P_s(1-\rho_j)}}{2\sqrt{N\sigma^2\rho_j}}\right). \end{aligned} \tag{6.35}$$

Proof: Please see Appendix C. ■

6.7.2 Mean secrecy rate for primary and secondary transmissions

Lemma 12. *The mean secrecy rate achievable at the legal receivers for primary and secondary transmissions can be obtained as*

$$\mathbb{E}_{\phi_e}[R_k|\gamma_k > \gamma_{E,k}] = \zeta(\log_2(1+\rho_k)^{1-P_{o_E,k}}$$

$$-\int_{\gamma_{min}}^{\rho_k} f_{\gamma_e}(x) \log_2(1+x))dx, \quad (6.36)$$

for the primary secrecy rate, $f_{\gamma_e}(x)$ can be written as

$$f_{\gamma_{pe}}(x) = -\frac{ae^b erfc(c)}{2x^{3/2}}, \quad (6.37)$$

where $a = \frac{\pi^{\frac{3}{2}}\lambda_e}{2}\sqrt{\frac{P_p}{N\sigma^2}}$, $b = \frac{\pi^3\lambda^2 P_s \exp(2/N^{-4})}{4\sigma^2}$, $c = \frac{\pi^{\frac{3}{2}}\lambda_e\sqrt{P_s}\exp(1/N^{-4})}{2\sqrt{\sigma^2}}$. For the secondary secrecy rate, $f_{\gamma_e}(x)$ can be obtained as

$$f_{\gamma_{se}}(x) = \frac{\pi^{3/2}a}{2\sqrt{\frac{1}{x}-1}x^3}\left(e^{\pi^2a^2\left(\frac{1}{x}-1\right)}\left(2\pi^2a^2(x-1)-x\right)\right. \left. erfc\left(\pi a\sqrt{\frac{1}{x}-1}\right)+2\sqrt{\pi}ax\sqrt{\frac{1}{x}-1}\right), \quad (6.38)$$

where $a = \frac{\lambda_e}{2}\sqrt{\frac{P_s}{N\sigma^2}}$. Furthermore, $k = i, \zeta = alpha$ for the primary transmissions or $k = j, \zeta = 1-\alpha$ for the secondary transmissions, $\gamma_{E,k}$ is the SINR of the central point with nearest location to the kth legal receiver.

Proof: Please see Appendix D. ■

6.8 The primary and secondary utility in Scenario II

The primary utility, denoted by U_{P_i}, can be written as

$$\begin{aligned} U_{P_i} &= R_i + c_p P_s \\ &= \alpha(\log_2(1+\rho_p)^{1-P_{o_{E,i}}} \\ &\quad -\int_{\gamma_{min}}^{\rho_p} f_{\gamma_{pe}}(x)\log_2(1+x)dx) + c_p P_s. \end{aligned} \quad (6.39)$$

Furthermore, the utility of the secondary transmission, denoted by U_{S_j}, can be written as

$$U_{S_j} = R_j - c_p P_s$$

$$= (1-\alpha)(\log_2(1+\rho_j)^{1-P_{o_E,j}} - \int_{\gamma_{min}}^{\rho_s} f_{\gamma_{se}}(x)\log_2(1+x)dx) - c_p P_s. \quad (6.40)$$

Based on matching theory, the following objective problem can be considered as the total secrecy rate (TSR_2) in Scenario II, by summing over the primary and secondary utilities:

$$TSR_2 = \sum_{i=1}^{N}\sum_{j=1}^{M} m_{i,j}(U_{P_i} + U_{S_j}), \quad (6.41)$$

where $m_{i,j} = 1$ if PT_i and ST_j are matched and $m_{i,j} = 0$ otherwise. It can be concluded that

$$TSR_2 = \sum_{i=1}^{N}\sum_{j=1}^{M} m_{i,j}(R_i + R_j). \quad (6.42)$$

Furthermore, the matching matrix that maximises the TSR_2 can be written as

$$M_2 = \arg \max_{m_{i,j}<1, i\in P, j\in S} \sum_{i=1}^{N}\sum_{j=1}^{M} m_{i,j}(R_i + R_j). \quad (6.43)$$

The PSMA can also be applied in Scenario II using the primary and secondary utilities in Equation (6.39) and Equation (6.40), respectively.

6.9 Numerical results and discussion

In this section, two scenarios are considered to highlight the effect of the PSMA algorithm on improving the secrecy rate.

i) Scenario I - Single eavesdropper: To evaluate the performance of the PSMA, three primary transmitter-receiver pairs, three secondary transmitter-receiver pairs, and one eavesdropper are considered, where the secondary transmitter nodes are located at coordinates (0m, 0m), (0m,10km) and (0m, 20km) and the corresponding receiver nodes are located at coordinates (10km,10km), (20km,10km) and (30km, 10km). The primary transmitter nodes are located at coordinates (-10km, 0km), (-10km,10km) and (-10km, 20km) and the corresponding receiver nodes are located at (10km, 0km), (10km, 10km) and(10km, 20km), based on the Cartesian coordinate system. Finally, the eavesdropper is located

at coordinate (35km,10km). Furthermore, it is assumed that $K = 2, M = 3, N = 3$, $\beta = 3$, and $\sigma^2 = 10^{-12}, c_p = 0.01$. To demonstrate the benefits of the PSMA, the performance of the proposed system is compared with the centralised algorithm in Equation (6.23). In the centralised algorithm, a centralised controller requires feedback between the PUs and SUs, which causes overhead that may affect the security of the system. Figure 6.2 indicates the average step size of the TSR versus the PT as α is increased or decreased. The proposed primary secrecy rate curves outperforms the centralised algorithm significantly when the step size is increased and converges to the centralised curve when the step size is reduced. In contrast, the secondary secrecy rate of the proposed system decreases slightly with increasing step size and approaches its corresponding value in the centralised curve when the step size approaches zero.

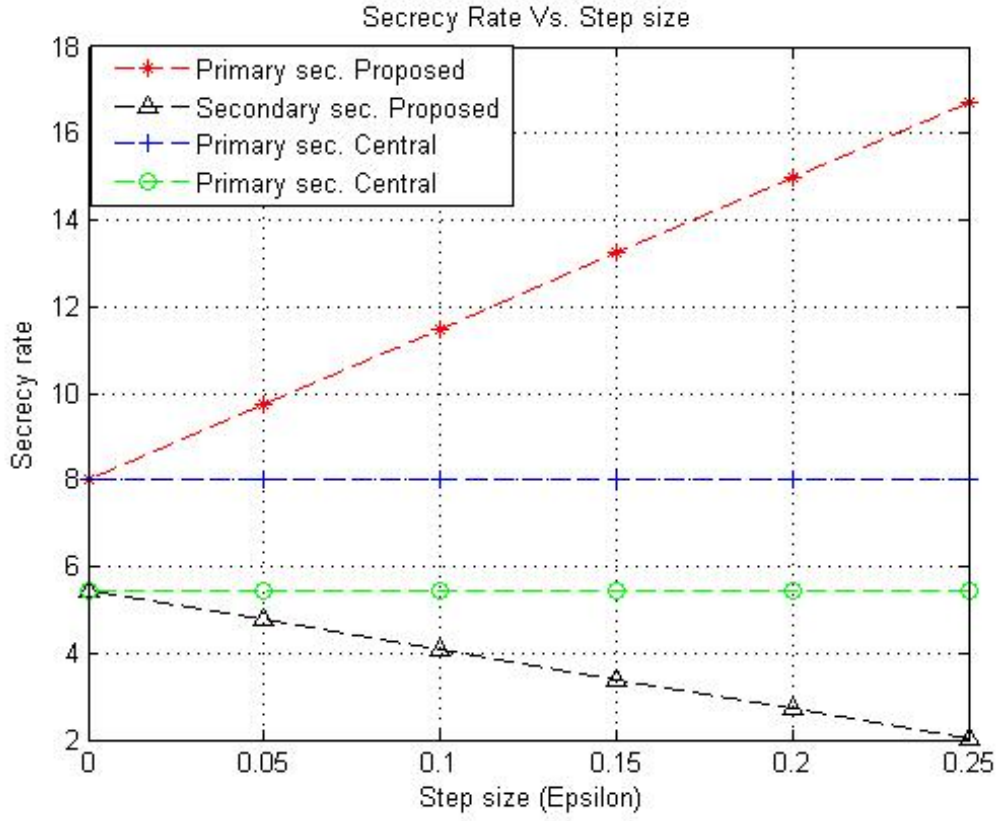

Figure 6.2: Secrecy rate vs. step size

ii) Scenario II - Multiple eavesdroppers: The secrecy outage probability and mean secrecy rate of the CR system are considered with multiple eavesdroppers. Here, it is assumed that $\lambda_e = 0.2, \sigma^2 = 10^{-6}$, $\rho_p = 1dB$, $\rho_s = -2dB$ and $\rho_{min} = -10dB$. Figure 6.5 shows the effect of the step size on the primary and secondary mean secrecy rates of the proposed system and those of the central algorithm. Notably, the primary and secondary mean secrecy rates increase with increasing step size. Additionally, the primary mean secrecy outage rate of the PSMA outperforms that of the central algorithm significantly, whereas the secondary secrecy rate is slightly reduced compared to that of the central algorithm.

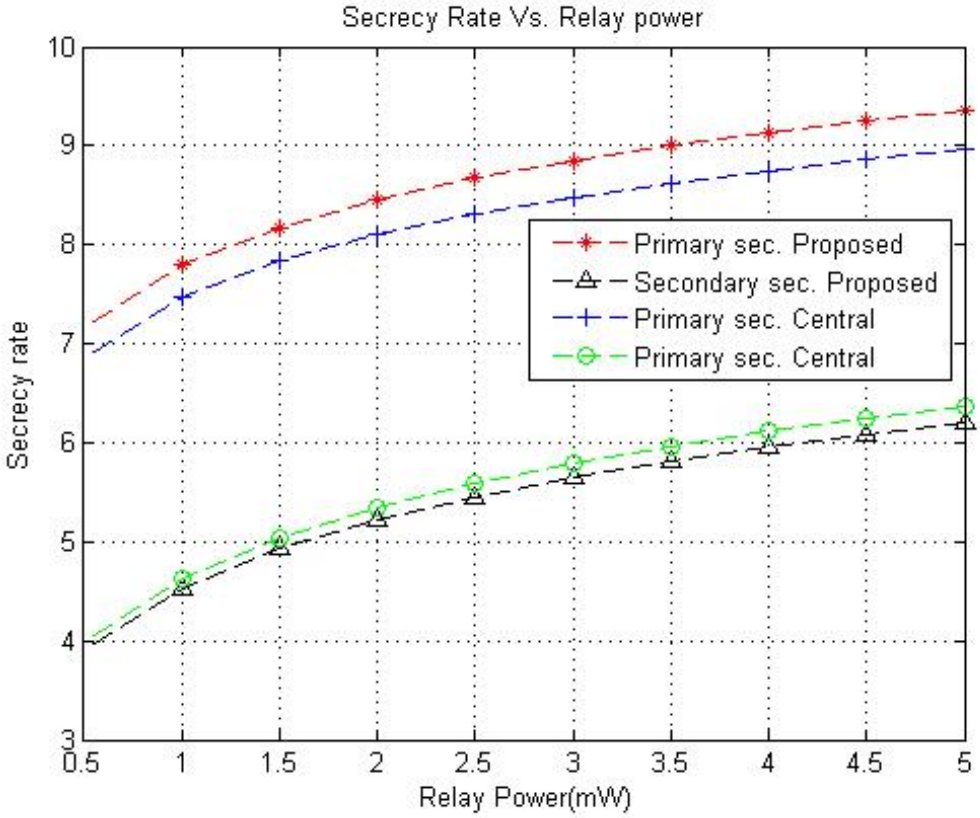

Figure 6.3: Secrecy rate vs. secondary power

Figure 6.3 indicates the effect of the secondary transmitter power on the secrecy rate of the proposed system when the step size is $\epsilon = 0.01$. The proposed PSMA performs significantly better than the central matching, and even more so for small

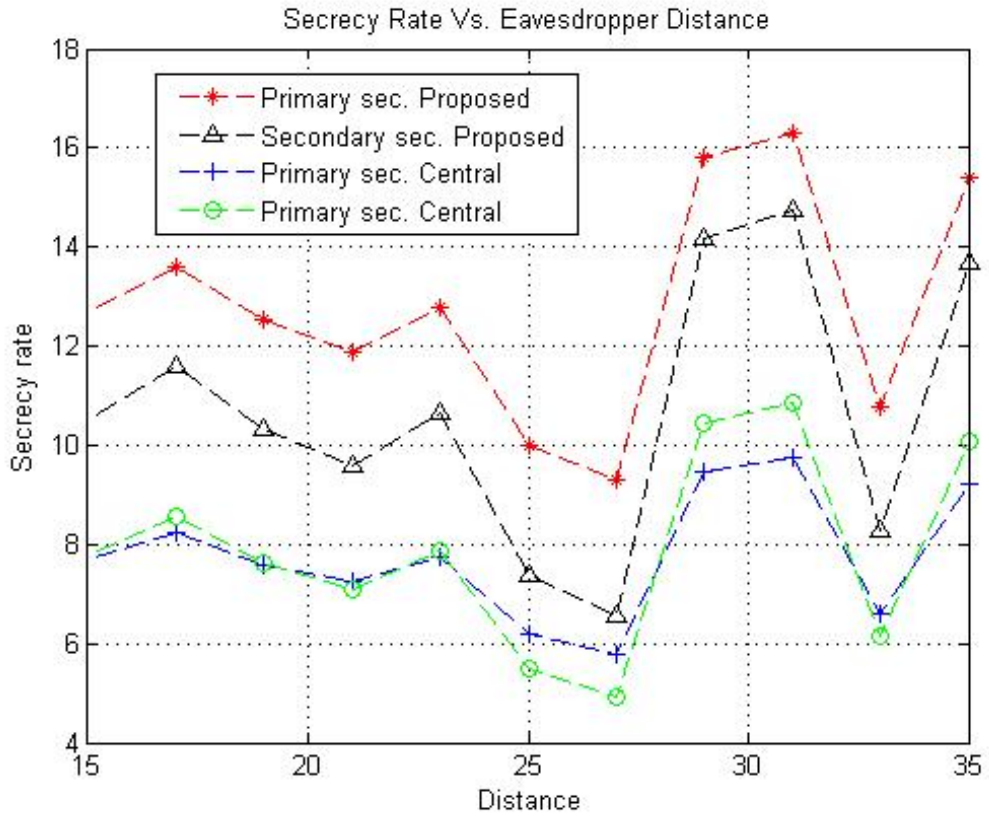

Figure 6.4: Secrecy rate vs. eavesdropper location

values of the secondary power. In contrast, the secondary secrecy rate is reduced slightly compared to the central curve. Figure 6.4 shows the effect of eavesdropper location on the secrecy rate of the proposed system when the step size is $\epsilon = 0.01$. For all eavesdropper locations, the proposed PSMA can achieve a significantly larger secrecy rate than central matching.

Figure 6.6 shows that primary secrecy rate increases significantly with increasing ρ_p, whereas the secondary secrecy rate is independent of ρ_p. Figure 6.7 indicates that the secondary secrecy rate increases significantly with increasing ρ_s and the primary secrecy rate is independent of ρ_s.

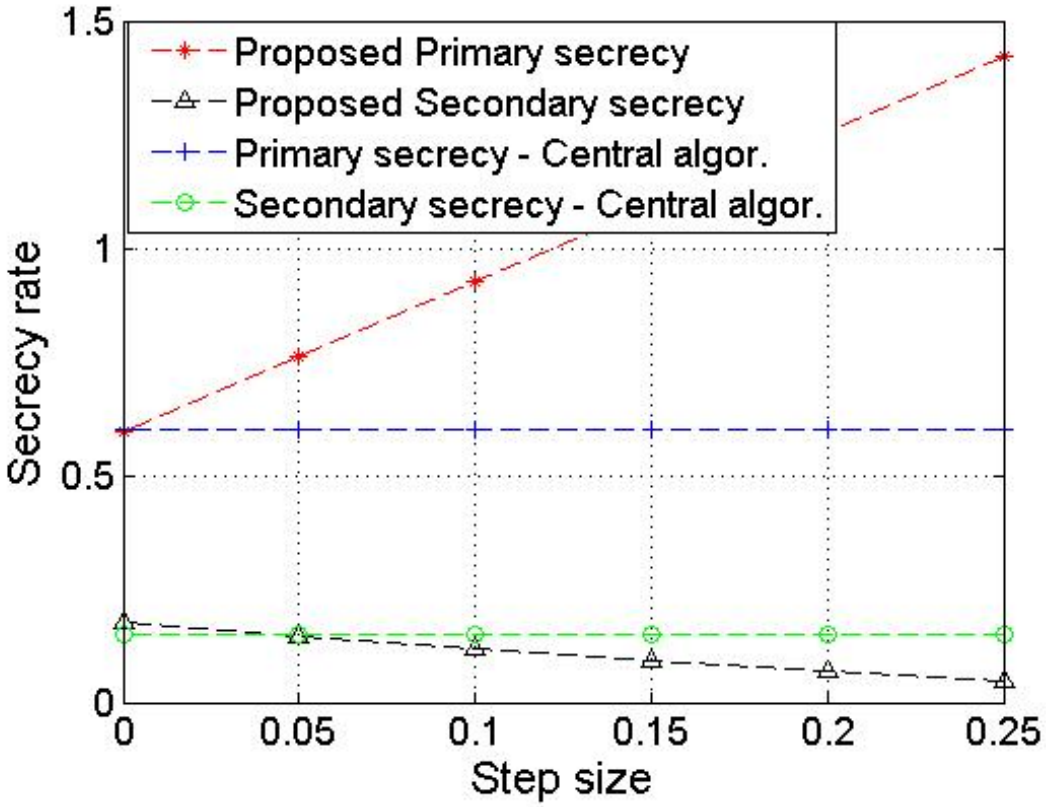

Figure 6.5: Secrecy rate vs. step size in Scenario II

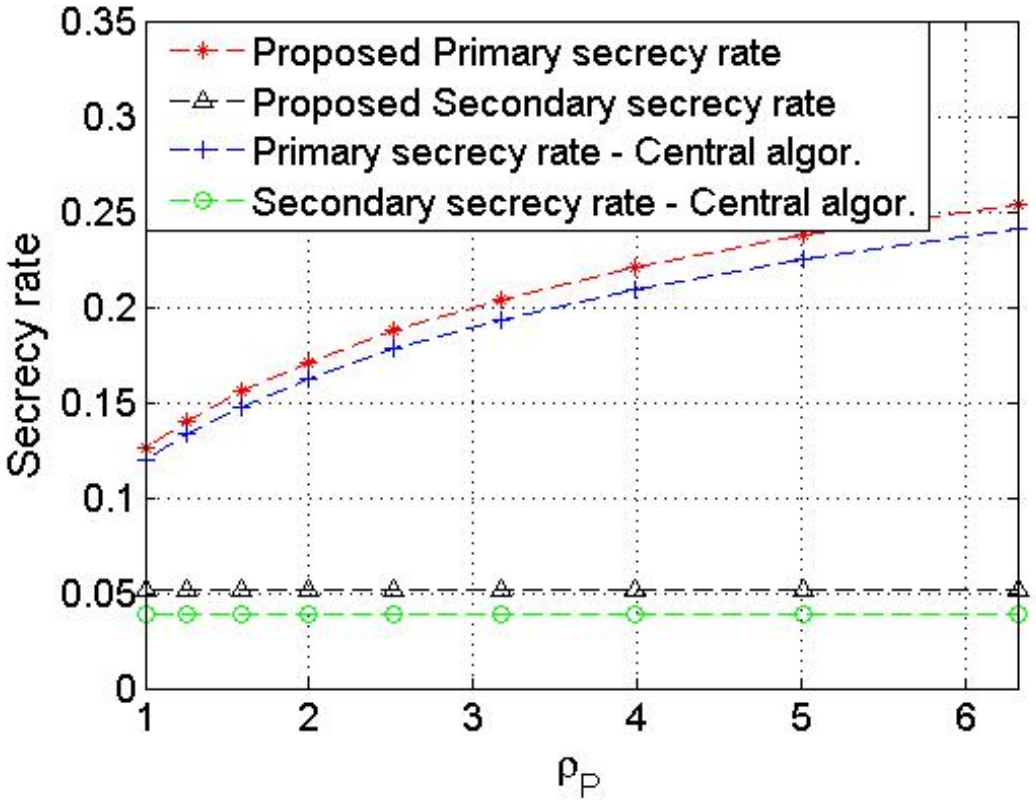

Figure 6.6: Secrecy rate vs. primary ρ_P in Scenario II

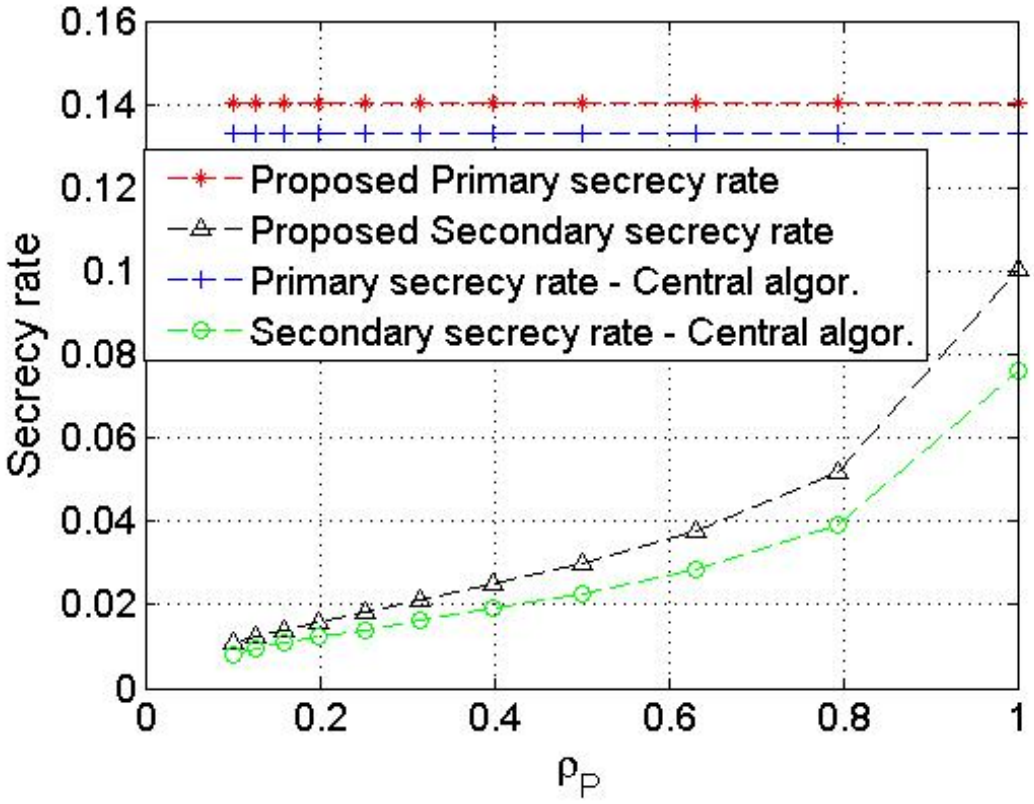

Figure 6.7: Secrecy rate vs. primary ρ_S in Scenario II

6.10 Conclusion

In this chapter, a cooperative spectrum-sharing approach has been proposed for a cognitive radio network consisting of multiple primary and secondary users. By introducing well-designed utility functions, the problem of partner selection was modelled as a one-to-one matching game that optimised the secrecy utility of both primary and secondary networks. This PSMA was then applied to two scenarios for a single eavesdropper and multiple eavesdroppers. The multiple eavesdroppers were assumed to be distributed according to a homogeneous PPP. To solve the presented matching game, a distributed algorithm (PSMA) was proposed, which produced a high secrecy rate that outperformed the centralised algorithm. Simulation results have shown that the proposed cooperative approach yields considerable gains in terms of the secrecy rate compared to the centralised algorithm.

Chapter 7

Conclusions and future work

The aim of this thesis was to investigate challenges to PHY security in CRNs. The thesis not only has contributed to the research community, but also has opened interesting areas for future research. Each chapter of the thesis has proposed a solution to an independent research problem, and hence the main contributions of the thesis are summarised below, along with concluding remarks, to create an overall picture of the research conducted.

Cooperative jamming was proposed to enhance primary secrecy rate, and a new chaos-based cost function was introduced in order to design a power control algorithm and analyse the dynamic spectrum-sharing issue in the uplink of cellular CRNs. For secondary users as the game-players in underlay scenarios, utility/cost functions were defined, taking into account the interference from and the interference tolerance of the primary users. The existence of the Nash equilibrium was proven for this power control game, which leads to significantly lower power consumption and a relatively fast convergence rate compared to existing game algorithms. Simulation results indicated that the primary secrecy rate is significantly improved by cooperative jamming and the proposed power control algorithm achieves low power consumption.

In addition, an integrated scheme was proposed with chaotic scrambling (CS), chaotic artificial noise, and a chaotic shift keying (CSK) scheme in an orthogonal

frequency division multiplexing (OFDM)-based CR system to enhance its physical layer security. By employing the chaos-based third-order Chebyshev map to achieve the optimum bit error rate (BER) performance of CSK modulation, the proposed three-layer integrated scheme was found to outperform the traditional OFDM system in an overlay scenario with a Rayleigh fading channel. Importantly, under three layers of encryption based on chaotic scrambling, chaotic artificial noise, and CSK modulation, a large key size can be generated to resist brute-force attacks and eavesdropping, leading to a significantly improved security rate.

Furthermore, a game theory-based cooperation scheme was investigated to enhance physical layer (PHY) security in both the primary and secondary transmissions of a cognitive radio network (CRN). In CRNs, the primary network may decide to lease its own spectrum for a fraction of time to the secondary nodes in exchange for appropriate remuneration. The secondary transmitter (ST) was considered as a trusted relay for primary transmission in the presence of the ED. The ST forwards a message from the primary transmitter (PT) in a decode-and-forward (DF) fashion and, at the same time, allows part of its available power to be used to transmit an artificial noise (i.e., jamming signal) to enhance secrecy rates. In order to allocate power between the message and jamming signals, a formulation and solution were presented for the optimisation problem for maximising the primary secrecy rate (PSR) and secondary secrecy rate (SSR) with malicious attempts from a single eavesdropper or multiple eavesdroppers. The cooperation between the primary and secondary transmitters was then analysed from a game-theoretic perspective, and their interaction was modelled as a Stackelberg game. The Stackelberg equilibrium was theoretically proven and computed. Finally, numerical examples were provided to illustrate the impact of the Stackelberg game-based optimisation on the achievable PSR and SSR. It was shown that spectrum leasing, based on trading secondary access for cooperation by means of relay and a jammer, is a promising framework for enhancing primary and secondary secrecy rates in cognitive radio networks when the ED can intercept both primary and secondary transmissions.

Finally, cooperative spectrum sharing was considered in a cognitive radio network consisting of multiple primary and multiple secondary users. A particular focus was the physical-layer security in cognitive radio networks wherein multiple secondary nodes assist multiple primary nodes in combating unwanted eavesdropping from a malicious eavesdroppers. Two scenarios were considered: a single eavesdropper and multiple eavesdroppers. In Scenario I, the secondary users play the game as a relay and jammer, whereas the secondary users play only as jammers in Scenario II. Multiple eavesdroppers are distributed according to a homogenous Poison point process (PPP). The primary and secondary secrecy rates were examined to find the solution of the developed matching game that yields a stable matching between the sets of the primary and secondary users. The closed forms for the outage probability and the mean secrecy rates for both the primary and secondary transmissions were derived. Furthermore, the saleability and convergence of matching theory were proved. Both the analytical and numerical results have shown that the proposed matching model is a promising approach under which the utility functions of both primary and secondary users are maximised.

The scope for future work in PHY security is extensive, and a few example directions are discussed here. Possibilities for applications of physical layer security techniques to commercially deployed wireless systems remain largely unexplored. The majority of the techniques discussed in this thesis, such as artificial noise for eavesdropper jamming and CSI-based precoding to optimise secrecy rates, are suitable for the underlying air interface (time/code/orthogonal frequency division multiple access). For example, an OFDMA-based base station may choose to transmit artificial noise along with data symbols in certain subcarriers, provided that spectral emission masks are not violated.

As physical layer security issues have been addressed and optimised in CRNs via matching theory, it is expected that new multi-user network scenarios and corresponding security schemes will continue to address and solve the security challenges in these networks. Secrecy challenges in massive MIMO systems, smart

grid systems, networks with simultaneous wireless information and power transfer, and heterogeneous networks should be specified and optimised via cooperative jamming and matching theory in future.

Bibliography

[1] FCC, ET Docket No 03-222, *Notice of proposed rule making and order,* Dec. 2003.

[2] S. Hakin, "Cognitive radio: Brain-empowered wireless communications", *IEEE Journal on Selected Areas in Communication.*, vol.23, no.2, pp. 201-220, Feb 2005.

[3] T. Weiss and F. Jondral, "Spectrum pooling: An innovative strategy for the enhancement of spectrum efficiency," *IEEE Communication Magazine*, vol. 42, no. 3, pp. 8-14, Mar. 2004.

[4] U. Berthold, F. Jondral, S. Brandes, and M. Schnell, "OFDM-based overlay systems: A promising approach for enhancing spectral efficiency [Topics in radio communications]," *IEEE Communication Magazine*, vol. 45, no. 12, pp. 52-58, Dec. 2007.

[5] S. Chuprun, J. Kleider, and C. Bergstrom, "Emerging software defined radio architectures supporting wireless high data rate OFDM," in *Proceeding of IEEE RAWCON*, 1999, pp. 117-120.

[6] A. T. Hoang and Y.-C. Liang, "Downlink channel assignment and power control for cognitive networks," *IEEE Transactions on Wireless Communication*, vol. 7, no. 8, pp. 3106-3117, Aug. 2008.

[7] P. Cheng, Z. Zhang, H.-H. Chen, and P. Qiu, "Optimal distributed joint frequency, rate and power allocation in cognitive OFDMA systems," *IET Communication*, vol. 2, no. 6, pp. 815-826, Jul. 2008.Stark,Medard

[8] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Transactions on Communication*, vol. 54, no. 7, pp. 1310-1322, Jul. 2006.

[9] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137:155, Jan. 2011.

[10] W. E. Stark and R. J. McEliece, "On the capacity of channels with block memory," *IEEE Trans. Inf. Theory,* vol. 34, no. 3, pp. 322-324, Mar. 1988.

[11] F. C. M. Lau and C. K. Tse, *Chaos-based digital communication systems*, Springer-Verlag, 2003.

[12] J. Yu and Y.-D. Yao, "Detection performance of chaotic spreading LPI waveforms," *IEEE Transactions on Wireless Communication*, vol. 4, no. 2, pp. 390-396, Mar. 2005.

[13] B. Le Saux, M. Helard, and P.-J. Bouvet, "Comparison of coherent and non-coherent space time schemes for frequency selective fast-varying channels," in *Proceeding of 2nd International Symposium on Wireless Communication Systems*, Sep. 2005, pp. 32-36.

[14] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "On secure OFDM system: Chaos based constellation scrambling," in *Proceeding of International Conference on Intelligent and Advanced Systems*, 2007.

[15] G. Kaddoum, F. Gagnon, and F.-D. Richardson, "Design of a secure Multi-Carrier DCSK system," in *Proceeding of the Ninth International Symposium on Wireless Communication Systems*, Jun. 2012.

[16] G. Kaddoum, M. Vu, and F. Gagnon, "Performance analysis of differential chaotic shift keying communications in mimo systems," in *Proceeding of IEEE International Symposium on Circuits and Systems (ISCAS)*, 2011, pp. 1580-1583.

[17] H.-O. Peitgen, H. Jrgens, and D. Saupe, *Chaos and fractals -new frontiers of science*, 2nd Edition, Springer-Verlag, 2004.

[18] Wai M. Tam, F. C. M. Lau, C. K. Tse, and A. J. Lawrance, "Exact analytical bit error rates for multiple access chaos-based communication systems," *IEEE Transactions on Circuits and Systems*, vol. 51, no. 9, Sep. 2004.

[19] A. J. Lawrance and G. Ohama "Exact calculation of bit error rates in communication systems with Chaotic modulation," *IEEE Transactions on Circuits and Systems*, vol. 50, no. 11, Nov.2003.

[20] H. Li, X. Wang, and W. Hou, "Secure transmission in OFDM systems by using time domain scrambling," in *Proceeding of 13th Canadian Workshop on Information Theory (CWIT)*, 2013.

[21] F. Lau, K. Cheong, and C. Tse, "Permutation-based DCSK and multiple access DCSK systems I: Fundamental Theory and Applications," *IEEE Transactions on Circuits and Systems*, vol. 50, pp. 733-742, 2003.

[22] S. Kaiser, "Multi-carrier CDMA mobile radio systems analysis and optimization of detection, decoding, and channel estimation," VOl-Verlag, Fortschittberichte, Ph.D. dissertation, 1998.

[23] S. Kondo and L. B. Milstein, "Multicarrier CDMA system with cochannel interference cancellation," *Proceeding of Vehicular Technology Conference* , Stockholm, Sweden, 1994.

[24] L.-L. Yang and L. Hanzo, "Performance of broadband multicarrier DSCDMA using space-time spreading-assisted transmit diversity," *IEEE Transactions on Wireless Communications*, vol. 4, no. 3, pp. 885-894, May 2005.

[25] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355:1387, 1975.

[26] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos I: Fundamental Theory and Applications, " *IEEE Transactions on Circuits and Systems*, vol. 47, pp. 1684-1691, 2000.

[27] W. M. Tam, F. C. M. Lau, C. K. Tse, and A, 1. Lawrance, "Exact analytical bit error rate for multiple access chaos-based communication systems I: Fundamental theory and applications," *IEEE Transactions on Circuits and Systems*, vol. 9, pp. 473-481, 2004.

[28] G. Kaddoum, P. Charge, D. Roviras, and D. Foumier-Prunaret, "A methodology for bit error rate prediction in chaos-based communication systems," *Springer, Birkhiiuser, Circuits, Systems and Signal Processing*, vol. 28, pp. 925-944, 2009.

[29] G. Kaddoum, F. Gagnon, F. Richardson, "Design of a secure Multi-Carrier DCSK system'" *Proceeding of international Symposium on Wireless Communication Syatems* (ISWCS) 2012.

[30] D. S. Swami and K. K. Sarma, "A logistic map based PN sequence generator for direct-sequence spread-spectrum modulation system", *Proceeding of International Conference on Signal Processing and Integrated Networks*, 2014.

[31] G. Geraci, S. Singh, J. G. Andrews, J. Yuan and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers",*IEEE Transactions on Wireless Communications*, vol.13, no.5, May 2014.

[32] D. Stroyan, W. Kendall, and J. Mecke, *Stochastic geometry and its applications*, Second Edition, John Wiley and Sons Ltd.,1996.

[33] M. Haenggi, "On distances in uniformly random networks," *IEEE Transaction on Information Theory*, vol.51, no. 10, pp.3584-3586, Oct. 2005.

[34] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal On Selected Areas in Communications*, vol. 27, no. 7, Sep. 2009.

[35] M. Medard, "Capacity of correlated jamming channels," in *Proc. 35th Allerton Conf.,* pp. 1043-1052, 1997.

[36] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. S. Shamai, and S. Verd, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604:619, Feb. 2009.

[37] Y. Liang, H. V. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, no.6, pp. 2470:2492, June 2008.

[38] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355:1387, 1975.

[39] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451:456, Jul. 1978.

[40] E. Tekin and A. Yener, "The general Gaussian multiple access and two way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735:2751, June 2008.

[41] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153:3167, May 2011.

[42] L. Dong ,H. Yousefizadeh and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper," *IEEE ICC Proceeding*, 2011.

[43] K. Lee,C. Chae, and J. Kang, "Spectrum Leasing via Cooperation for Enhanced Physical-Layer Secrecy" *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, November 2013.

[44] Z. Chu, K. Cumanan, Z. Ding, M. Johnston and S. Le Goff,"Secrecy Rate Optimizations for a MIMO Secrecy Channel with a Cooperative Jammer," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, May 2015.

[45] Frdric Gabry, Nan Li, Nicolas Schrammar, Maksym Girnyk, Lars K. Rasmussen and Mikael Skoglund," On the Optimization of the Secondary Transmitters Strategy in Cognitive Radio Channels with Secrecy," *IEEE Journal on selected areas in Communications*, vol.32, no.3, March 2014.

[46] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153:3167, May 2011.

[47] Ning Zhang, Ning Lu, Nan Cheng, Jon W. Mark, Xuemin (Sherman) Shen,"Cooperative Spectrum Access Towards Secure Information Transfer for CRNs,"*IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, March 2013.

[48] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. S. Shamai, and S. Verd, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604:619, Feb. 2009.

[49] H. G. Bafghi, S. Salimi, B. Seyfe, and M. Aref, "Cognitive interference channel with two confidential messages," in Proc. *IEEE Int. Symp. Inf. Theory Appl. (ISITA)*, Oct. 2010.

[50] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tutorials*, vol. 15, no. 1, pp. 428-445, 2013.

[51] T. C. Clancy and N. Goergen,"Security in cognitive radio networks: Threats and mitigation," in *Proc. CrownCom,* pp. 1-8, May 2008.

[52] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerailities and protection countermeasures: a multi-dimensional analysis and assessment," in *Proc. IEEE CrownCom*, pp. 456-464, Aug. 2007.

[53] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," in *Proc. IEEE CrownCom*, May 2008.

[54] Y. Pei, Y. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494-1592 , Apr. 2010.

[55] Y. Wu and K. Liu, "An information secrecy game in cognitive radio networks,"*IEEE Trans. Inf. Forens. Security*, vol. 6, no. 3, pp. 831-842, Sep. 2011.

[56] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming,"*IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134-145, Jan. 2013.

[57] A. Garnaev and W. Trappe, "An eavesdropping game with SINR as an objective function," in *Proc. SECURECOMM*, pp.142-162, 2009.

[58] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818-830, Sep. 2011.

[59] A. Mukherjee and A. L. Swindlehurst, "Equilibrium outcomes of dynamic games in MIMO channels with active eavesdroppers," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010.

[60] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper,"*IEEE Trans. Signal Process.*, vol. 61, no. 1, pg. 82-91, Jan. 2013.

[61] J. Xie and S. Ulukus, "Secrecy games on the one-sided interference channel," in *Proc. IEEE ISIT*, July 2011.

[62] M. Ara, H. Reboredo, S. Ghanem and M. R. D. Rodrigues, "A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer," in *Proc. IEEE ICCS*, Singapore, Nov. 2012.

[63] W. Saad, Z. Han, M. Debbah, A. Hjrungnes, and T. Basar,"Physical layer security: Coalitional games for distributed cooperation," in *Proc. 7th WiOpt*, 2009.

[64] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multihop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980-3991, Nov. 2012.

[65] Z. Han, N. Marina, M. Debbah, and A. Hjrungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer", *Eurasip J. Wireless Commun. and Network.*, 2009.

[66] Z. Han, N. Marina, M. Debbah, and A. Hjrungnes, "Improved wireless secrecy capacity using distributed auction theory", in *Proc. 5th ICMAS, China*, 2009.

[67] S. Anand and R. Chandramouli, "Secrecy capacity of multi-terminal networks with pricing," [Online]. Available: http://koala.ece.stevenstech. edu/ mouli/IT02.pdf.

[68] J. Cho, Y.-W. P. Hong, and C.-C. J. Kuo, "A game theoretic approach to eavesdropper cooperation in MISO wireless networks," in *Proc. IEEE ICASSP*, 2011.

[69] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal,* vol. 28, pp. 656-715, 1949.

[70] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "New results on multipleinput multiple-output broadcast channels with confidential messages," *IEEE Trans. Inf. Theory,* vol. 59, no. 3, pp. 1346-1359, Mar. 2013.

[71] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT, Seattle,* July 2006.

[72] A. B. Carleial and M. Hellman, "A note on Wyners wiretap channel," *IEEE Trans. Inf. Theory,* vol. 23, no. 5, pp. 625-627, May 1977.

[73] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels,"' *IEEE Trans. Inf. Theory,* vol. 57, no. 1, pp. 137-155, Jan. 2011.

[74] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. S. Shamai, and S. Verd, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604-619, Feb. 2009.

[75] A. Wyner, '"The wire-tap channel," *Bell Systems Technical J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[76] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[77] A. Goldsmith, S. A. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 684-702, Jun. 2003.

[78] J. Huang and A. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696-1707, Apr. 2012.

[79] J.Huang and A. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[80] M. Dehghan, D.Goeckel, M.Ghaderi, and Z.Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3025-3029, Sep. 2012.

[81] H.-M. Wang, M. Luo, X. G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure A F relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39-42, Jan. 2013.

[82] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEETrans. Inf. Theory,* vol. 58, no. 3, pp. 1594-1611, Mar. 2012.

[83] Y. Liang, H. V. Poor, and L. Ying, "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 682-692, Sep. 2011.

[84] J. Vilela, P. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *IEEE Trans. Inf. Forensics Security* vol. 6, no. 3, pp. 616-627, Sep. 2011.

[85] E. A. Jorswieck and R. Mochaourab, "Secrecy rate region of MISO interference channel: Pareto boundary and non-cooperative games," *Proc. Int. IT Workshop on Smart Antennas (WSA)*, Berlin, Germany, Feb. 2009.

[86] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wire tap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[87] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," *Proc. IEEE Int. Symp. Inform.Theory (ISIT)*, Nice, France, Jun. 2007, pp. 2466-2470.

[88] J. Huang and, A. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[89] L. Feng and W. Li, "A new game algorithm for power control in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol.60, no. 9, Nov. 2011.

[90] R. W. Nettleton and H. Alavi, "Power control for spread spectrum cellular mobile radio system," in *Proc. IEEE Vehicular Technology Conference*, vol. 33, pp. 242-246, 1983.

[91] S. Koskie and Z. Gajic, "A Nash game algorithm for SIR-based power control in 3G wireless CDMA networks," *IEEE/ACM Trans. Networking*, vol. 13, pp. 1017-1026, 2005.

[92] L. Junyou and Z. Junhui, "An improved wireless location algorithm based on Chaos optimization algorithm," in *Proc. Int. Conf. on Wireless Communications, Networking and Mobile Computing*, pp. 885-889, Sep. 2007.

[93] E. Pasandshanjani, B. H. Khalaj, and M. S. Moghaddam, "A new cost function for game theoretic SIR-based power control algorithms," in *Proc. 7th Int. Conf on Wireless Communications and Mobile Computing (IWCMC)*, Jul. 2011.

[94] P. J. Smith, P. A. Dmochowski, H. A. Suraweera, and M. Shafi, "The effects of limited channel knowledge on cognitive radio system capacity," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, Feb. 2013.

[95] K. Lee,C. Chae, and J. Kang, "Spectrum Leasing via Cooperation for Enhanced Physical-Layer Secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, Nov.2013.

[96] E. Tekin and A. Yener, "The general Gaussian multiple access and two way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735:2751, June 2008.

[97] M. haenggi, Jeffry G. Andrews, Francois Baccelli, Olivier Dousse and Massimo Franceschetti," Stochastic Geometry and Random Graphs for the analysis and Design of Wireless Networks," *IEEE Journal On Selected Areas In Communications*, vol. 27, no. 7, September 2009.

[98] Frdric Gabry, Nan Li, Nicolas Schrammar, Maksym Girnyk, Lars K. Rasmussen and Mikael Skoglund," On the Optimization of the Secondary Transmitters Strategy in Cognitive Radio Channels with Secrecy,"*IEEE Journal on selected areas in Communications*, vol.32, no.3, March 2014.

[99] Ning Zhang, Ning Lu, Nan Cheng, Jon W. Mark, Xuemin (Sherman) Shen,"Cooperative Spectrum Access Towards Secure Information Transfer for CRNs,"*IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, March 2013.

[100] I. Stanojev and A. Yener,"Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming,"*IEEE Transactions on Wireless Communications*, vol. 12, no. 1, January 2013.

[101] E. Toher, O. O. Koyluoglu, and H. El Gamal, "Secrecy games over the cognitive channel,"in Proc. *IEEE Int. Symp. Inf. Theory (ISIT)*, 2010.

[102] Z. Han and K. J. R. Liu, "Non-cooperative power-control game and throughput game over wireless networks,"*IEEE Transactions on Communications*, vol. 53, no. 10, pp. 1625:1629, Oct. 2005.

[103] Resource Allocation for Wireless Networks: Basics, Techniques and Applications. *Cambridge University Press*, 2008.

[104] M. Simaan and J. B. Cruz, "On the Stackelberg strategy in non zero sum games," *Journal Optimization Theory Application*, vol. 11, no. 5, pp. 533:555, May 1973.

[105] I. Stanojev and A. Yener, "Cooperative jamming via spectrum leasing," in Proc. *IEEE International Symp. Modeling Optimization Mobile, Ad Hoc Wireless Netw. (Wiopt)*, May 2011.

[106] Giovani Geraci,Sarabjot Singh, Jeffrey G.Andrews,Jinhong Yuan and Iain B. Collings"Secrecy rates in broadcast channels with confidential messages and

external eavesdroppers"*IEEE Transactions on Wireless Communications*, vol. 13, no. 5, May 2014.

[107] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, and T. Basar, "Physical layer security: Coalitional games for distributed cooperation," in Proc. *7th international symposium on Wiopt*, 2009.

[108] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multihop networks," *IEEE Trans. Wireless Communications*, vol. 11, no. 11, pp. 3980:3991, Nov. 2012.

[109] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *Eurasip J. Wireless Communications and Network.*, 2009.

[110] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Improved wireless secrecy capacity using distributed auction theory," in Proc. *5th ICMAS*, China, 2009.

[111] S. Anand and R. Chandramouli, "Secrecy capacity of multi-terminal networks with pricing,"[Online]. Available: *http://koala.ece.stevenstech.edu/mouli/IT02.pdf.*

[112] S. A. A. Fakoorian and A. L. Swindlehurst, "MIMO interference channel with confidential messages: game theoretic beamforming designs," in Proc. *Asilomar Conference on Signals, Systems, and Computers*, November 2010.

[113] S. A. A. Fakoorian and A. L. Swindlehurst, "Competing for secrecy in the MISO interference channel," *IEEE Trans. Signal. Process.*, vol. 61, no. 1, pp. 170:181, Jan. 2013

[114] J. Cho, Y.-W. P. Hong, and C.-C. J. Kuo, "A game theoretic approach to eavesdropper cooperation in MISO wireless networks," in Proc. *IEEE ICASSP*, 2011.

[115] Yongle Wu and K. J. Ray Liu,"An Information Secrecy Game in Cognitive Radio Networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, September 2011.

[116] Frdric Gabry, Alessio Zappone, Ragnar Thobaben, Eduard A. Jorswieck and Mikael Skoglund,"Energy Efficiency Analysis of Cooperative Jamming in Cognitive Radio Networks With Secrecy Constraints ,"*IEEE Wireless Communications Letters*, vol.4, no.4, August 2015.

[117] L. Dong ,H. Yousefizadeh and H. Jafarkhani, "Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper,"*Proc. IEEE ICC*,2011.

[118] G. Kim,"Scheduling in wireless ad hoc networks: algorithms with performance guarantees". *ProQuest*, 2008.

[119] Hong Xing, Liang Liu and Rui Zhang,"Secrecy Wireless Information and Power Transfer in Fading Wiretap Channel,"*IEEE Transactions on Vehicular Technology*, Vol. pp, No. 99, Jan. 2015.

[120] Havish Koorapaty, Amer A. Hassan and Sandeep Chennakeshu "Secure Information Transmission for Mobile Radio"*IEEE Communication Letters*, Vol.4, No.2, Feb. 2000.

[121] Jun Yang,Il-Min Kim,and Dong In Kim," Optimal Cooperative Jamming for Multiuser Broadcast Channel with Multiple Eavesdroppers,"*IEEE Trans. Wireless Communications*, vol. 12, no. 6, June 2013.

[122] Q. Ma and C. Tepedelenlioglu, "Antenna selection for spacetime coded systems with imperfect channel estimation," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 710:719, Feb. 2007.

[123] W. M. Gifford, M. Z. Win, and M. Chiani, "Diversity with practical channel estimation,"*IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1935:1947, Jul. 2005.

[124] J. O. Neel, "Analysis and design of cognitive radio networks and distributed radio resource management algorithms," Ph.D. dissertation, Virginia Polytechnic Institute, Sep. 2006.

List of publications

Journal papers

1. Ali Al Talabani, Arumugam Nallanathan, and Huan X. Nguyen. "A novel chaos-based cost function for power control of cognitive radio networks," *IEEE Communication Letters,* vol. 19, no. 4, April 2015.

2. Ali Al Talabani, Yansha Deng, Arumugam Nallanathan, and Huan X. Nguyen. "Enhancing the secrecy rate in cognitive radio via a multi-level Stackelberg game," *IEEE Communication Letters*, forthcoming in 2016.

3. Ali Al Talabani, Yansha Deng, Arumugam Nallanathan, and Huan X. Nguyen. "Enhancing the secrecy rate in cognitive radio networks via a Stackelberg game," *IEEE Transactions on Communications*, under review.

4. Ali Al Talabani, Yansha Deng, Arumugam Nallanathan and Huan X. Nguyen. "On the physical layer security of a cognitive radio transceiver via chaotic OFDM," *IEEE Transactions on Communications*, under review.

5. Ali Al-Talabani, Arumugam Nallanathan, S. Lambotharan "Physical Layer Security of Cognitive Radio Networks via Matching Theory," *IEEE JSAC Special Issue on Game Theory for Networks,* under review.

Conference papers

1. Ali Al Talabani, Arumugam Nallanathan, and Huan X. Nguyen. "Enhancing physical layer security of cognitive radio transceiver via chaotic OFDM," *Proc.*

IEEE ICC, Signal Processing for Communications Symposium, London, June 2015, pp. 4805-4810.

2. Ali Al Talabani, Arumugam Nallanathan, and Huan X. Nguyen. "Enhancing secrecy rate in cognitive radio via game theory," *Proc. IEEE Globe Comm.*, Signal Processing Symposium, December 2015, forthcoming.

3. Ali Al Talabani, Yansha Deng, Arumugam Nallanathan, and Huan X. Nguyen. "Enhancing physical layer security of cognitive radio networks via distributive matching theory," *IEEE Globe Comm. Conference*, 2016, submitted.

Appendix A

Proofs from Chapter 4

A.1 Proof of Lemma 1

In order to prove the concavity of the primary transmission's utility, the second derivative of Eq. (4.33) with respect to ϵ_1 is derived as follows:

$$\frac{\partial^2 R_{sec}}{\partial^2 \epsilon} = \left(-\frac{\rho_{ss}^2}{(1+\epsilon\rho_{ss})^2} - \frac{\rho_{se}^2}{(1+(1-\epsilon)\rho_{se})^2}) \right). \tag{A.1}$$

The second derivative in Eq. (A.1) is negative and hence the secrecy rate of secondary transmission is concave in terms of ϵ.

A.2 Proof of Lemma 2

Following Lemma 1 in [31], the secrecy outage probability of the kth ST due to the most malicious eavesdropper ($\gamma_{E,k} = \max \gamma_{e,k}$) is presented as follows:

$$\begin{aligned} P_{o,k} &= \mathbb{P}(\gamma_{E,k} \geq \gamma_k | \gamma_k) \\ &= 1 - \mathbb{E}_{\phi_e} \left[\prod_{x \in \phi_e} \mathbb{P}(\gamma_{x,k} < \gamma_k | \gamma_k) \right] \\ &= 1 - \mathbb{E}_{\phi_e} \left[\prod_{x \in \phi_e} [1 - \mathbb{P}(\gamma_{x,k} \geq \gamma_k | \gamma_k)] \right] \\ &= 1 - \mathbb{E}_{\phi_e} \left[\prod_{x \in \phi_e} [1 - \mathbb{P}(\epsilon P_s |h_{se}|^2 \geq (\sigma^2 d_{x,k}^{\alpha} \right. \end{aligned}$$

$$
\begin{aligned}
& +(1-\epsilon)P_s\left|h_{se}\right|^2)\gamma_k)]] \\
= \; & 1-\mathbb{E}_{\phi_e}\left[\prod_{x\in\phi_e}[1-\mathbb{P}(|h_{se}|^2 \geq \gamma_k N\sigma^2 d_{x,k}^{\alpha}\right. \\
& \left. +(\epsilon-(1-\epsilon)\gamma_k)P_s]\right] \\
= \; & 1-\mathbb{E}_{\phi_e}\left[\prod_{x\in\phi_e}[1- \right. \\
& \left. \exp(-\frac{N\gamma_k\sigma^2|x|^{\alpha}}{(\epsilon-(1-\epsilon)\gamma_k)P_s})]\right] \qquad \text{(A.2)} \\
= \; & 1-\exp\left[-2\pi\lambda_e\int_0^{\infty} z\exp(-\frac{N\gamma_k\sigma^2|x|^{\alpha}}{}\right. \\
& \left. \frac{}{(\epsilon-(1-\epsilon)\gamma_k)P_s})dz\right] \qquad \text{(A.3)} \\
= \; & 1-\exp\left[-\pi\lambda_e\int_0^{\infty}\exp(-\frac{N\gamma_k\sigma^2 y^{\alpha/2}}{}\right. \\
& \left. \frac{}{(\epsilon-(1-\epsilon)\gamma_k)P_s})dy\right] \qquad \text{(A.4)} \\
= \; & 1-\exp\left[-\frac{2\pi\lambda_e}{\alpha(\frac{N\gamma_k\sigma^2}{(\epsilon-(1-\epsilon)\gamma_k)P_s})^{\frac{2}{\alpha}}}\right. \\
& \left. \int_0^{\infty} e^{-t}t^{\frac{2}{\alpha}-1}dt\right] \qquad \text{(A.5)} \\
= \; & 1-\exp\left[\frac{2\pi\lambda_e}{\alpha(\frac{N\gamma_k\sigma^2}{(\epsilon-(1-\epsilon)\gamma_k)P_s})^{\frac{2}{\alpha}}}\Gamma(\frac{2}{\alpha})\right], \\
& \qquad \text{(A.6)}
\end{aligned}
$$

where Eq. (A.2) is achieved according to the PPP distribution of eavesdroppers [33]. In Eq. (A.3), it is possible to replace $|z| = y$ and apply the probability generating functional (PGFL) for the PPP ϕ_e, given by [32] as

$$\mathbb{E}_{\phi_e}\left[\prod_{x\in\phi_e} f(x)\right] = \exp\left(-\int_{\mathbb{R}^2}[1-f(x)]\lambda_e dx\right).$$

In addition to converting to polar coordinates, $y = z^2$ is substituted in Eq. (A.4), and Eq. (A.5) follows from the fact that the allocated secondary power $P_s(1-\epsilon)$ is independent from the PPP distribution of eavesdroppers and $t = \frac{N\gamma_k\sigma^2 y^{\alpha/2}}{(\epsilon-(1-\epsilon)\gamma_k)P_s}$. Finally, Eq. (A.6) emerges from the definition of the Gamma function.

A.3 Proof of Lemma 3

The secrecy outage probability at the kth SR due to the nearest eavesdropper is presented as the following:

$$\begin{aligned}
P_{o_E,k} &= \int_0^\infty \mathbb{P}(\gamma_E, k \geq \gamma_k | \gamma_k, |d_{E_0,k}| = x) f_E(x) dx \\
&= \int_0^\infty \left[\exp(-\frac{N\gamma_k \sigma^2 x^\alpha}{(\epsilon - (1-\epsilon)\gamma_k) P_s}) f_E(x) dx \right] && \text{(A.7)} \\
&= 2\pi\lambda_e \int_0^\infty \Big[x \exp(-\frac{N\gamma_k \sigma^2 x^\alpha}{(\epsilon - (1-\epsilon)\gamma_k) P_s} \\
&\quad -\lambda_e \pi x^2) dx \Big] && \text{(A.8)} \\
&= 2\pi\lambda_e \int_0^\infty \Big[x \exp(-\frac{N\gamma_k \sigma^2 x^4}{(\epsilon - (1-\epsilon)\gamma_k) P_s} \\
&\quad -\lambda_e \pi x^2) dx \Big] && \text{(A.9)} \\
&= \pi\lambda_e \int_0^\infty \Big[\exp(\frac{N\gamma_k \sigma^2 u^2}{(\epsilon - (1-\epsilon)\gamma_k) P_s} \\
&\quad - \lambda_e \pi u) du \Big] && \text{(A.10)} \\
&= \frac{\pi^{3/2}\lambda_e}{2\sqrt{\frac{N\gamma_k\sigma^2}{(\epsilon-(1-\epsilon)\gamma_k)P_s}}} \exp\left[\frac{\pi^2 {\lambda_e}^2}{\frac{4N\gamma_k\sigma^2}{(\epsilon-(1-\epsilon)\gamma_k)P_s}} \right] \\
&\quad \operatorname{erfc}\left(\frac{\pi\lambda_e}{2\sqrt{\frac{N\gamma_k\sigma^2}{(\epsilon-(1-\epsilon)\gamma_k)P_s}}} \right), && \text{(A.11)}
\end{aligned}$$

where Eq. (A.7) follows from the PPP distribution of eavesdroppers. According to [33] and [34], Eq. (A.8) holds when the distance between the kth ST and the nearest eavesdropper follows

$$f_E(x) = 2\lambda_e \pi x \exp(-\lambda_e \pi x^2).$$

In Eq. (A.9), let $\alpha = 4$, while $u = x^2$ is used to obtain Eq. (A.10). Eq. (A.11) is then obtained by the following formula:

$$\int_0^\infty \exp(-bx^2 - cx) dx = \frac{1}{2}\sqrt{\frac{\pi}{b}} \exp(\frac{c^2}{4b}) \operatorname{erfc}\left(\frac{c}{2\sqrt{b}} \right).$$

A.4 Proof of Lemma 4

The mean secrecy rate when $\gamma_k > \gamma_{e,k}$ is presented as follows:

$$\mathbb{E}_{\phi_e}[R_k | \gamma_k > \gamma_{e,k}] = \mathbb{E}_{\phi_e}[\max[\log_2(1 + \gamma_k)$$

$$
\begin{aligned}
& - \log_2(1 + \max_e \gamma_{e,k})]\Big] \\
= \; & \mathbb{E}_{\phi_e}\left[\log_2(1+\gamma_k)\right. \\
& \left. - \log_2(1 + \max_e \gamma_{e,k})\right] \mathbb{1}_{(\gamma_{e,k}<\gamma_k)} \\
= \; & \mathbb{E}_{\phi_e} \log_2(1+\gamma_k)\mathbb{1}_{(\gamma_{e_0,k}<\gamma_k)} - \mathbb{E}_{\phi_e} \\
& \log_2(1+\gamma_{e_0,k})\mathbb{1}_{(\gamma_{min}<\gamma_{e_0,k}<\gamma_k)}
\end{aligned} \tag{A.12}
$$

$$
\begin{aligned}
= \; & \mathbb{P}(\gamma_{e_0,k} < \gamma_k) \log_2(1+\gamma_{e_0,k}) \\
& -\mathbb{P}(\gamma_{min} < \gamma_{e_0,k} < \gamma_k) \\
& \log_2(1+\gamma_{e_0,k})
\end{aligned} \tag{A.13}
$$

$$
\begin{aligned}
= \; & \log_2(1+\gamma_k)^{1-P_{o_E,k}} \\
& - \int_{\gamma_{min}}^{\gamma_k} f_{\gamma_{e_0,k}}(y) \log_2(1+y) dy,
\end{aligned} \tag{A.14}
$$

where $\mathbb{1}_{(.)}$ is an indicator function. Eq. (C.10) considers the worst case of eavesdropping by $\gamma_{e_0,k}$, which is bounded by γ_{min} and γ_k. Eq. (A.14) follows from the distribution function of $\gamma_{e_0,k}$, which is $f_{\gamma_{e_0,k}}(x) = \frac{\partial \mathbb{P}(\gamma_{E,k}<\gamma_k)}{\partial x}$ [31].

Appendix B

Proofs from Chapter 5

B.1 Proof of Lemma 1

In order to prove the concavity of the secondary transmission utility, the second derivative of Eq. (6.16) with respect to ϵ is derived as

$$\frac{\partial^2 U_{SSEC}}{\partial^2 \epsilon} = q\left(-\frac{\rho_{ss}^2}{(1+\epsilon\rho_{ss})^2} - \frac{\rho_{se}^2}{(1+(1-\epsilon)\rho_{se})^2}\right), \tag{B.1}$$

where $q = \alpha(1-\beta)/(\ln 2)$. It is evident that the second derivative in Eq. (B.1) is negative. Thus, the utility of the secondary transmission is concave in terms of ϵ.

B.2 Proof of Lemma 2

As all eavesdroppers are uniformly distributed around the ST and SR, it can be assumed that

$$|h_{se,1}| = |h_{se,2}| = ... = |h_{se,L}|$$

which leads to

$$\rho_{se,1} = \rho_{se,2} = ... = \rho_{se,L} = \rho_{se}.$$

Also, it is assumed that

$$|h_{re,1}| = |h_{re,2}| = ... = |h_{re,L}|.$$

Therefore, the achievable U_{SSEC} is written as

$$\begin{aligned} U_{SSEC} &= R_{ssec} - k\epsilon = R_{ss} - R_{se} - k\epsilon \\ &= \alpha(1-\beta)(\log_2(1+\epsilon\rho_{ss}) - \log_2(1+ \\ &\qquad \frac{\epsilon P_s h_{se}}{\sigma^2 + P_J \left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right| + (1-\epsilon)P_s h_{se}}) \Bigg) \\ &\qquad - k\epsilon. \end{aligned} \tag{B.2}$$

In order to prove the concavity of the utility of the secondary transmission, the second derivative of Eq. (B.2) is derived with respect to ϵ as

$$\begin{aligned} \frac{\partial^2 U_{SSEC}}{\partial^2 \epsilon} &= q\left(\frac{-\rho_{ss}^2}{(1+\epsilon\rho_{ss})^2} + \right. \\ &\qquad \frac{-L\rho_{se}^2}{1+\frac{P_J\left|\mathbf{h}_{re}^{\dagger}\mathbf{W}_J\mathbf{h}_{re}\right|}{\sigma^2}} \\ &\qquad \left. \frac{}{+(1-\epsilon)\rho_{se}}\right), \end{aligned} \tag{B.3}$$

where $q = \alpha(1-\beta)/2\ln 2$. The second derivative in Eq. (B.3) is negative, and therefore the utility of the secondary transmission in colluding eavesdroppers is concave in terms of ϵ.

Appendix C

Proofs from Chapter 6

C.1 Proof of Lemma 1

To prove that the matching produced by the PSMA is not blocked by an individual, it is first noted that

- each relay will never receive a negative utility because, according to step 1-a in the PSMA, the minimum offer is α_{min}; and
- each PT will only match with the ST in its demand set.

It will now be proven by contradiction that the matching produced by the PSMA will not result in any blocking pairs. Defining the matching function of the PSMA as ψ, it is assumed that PT_{i^b} and ST_{j^b} constitute a blocking pair. This implies that there exists a α_{i^b,j^b} such that

$$U_{P_{j^b,i^b}} > U_{P_{j,\psi(j)}} \tag{C.1}$$

and

$$U_{S_{j^b}} > U_{S_{\psi(i)}}. \tag{C.2}$$

The following two conclusions can be drawn:

(C1): As U_{S_j} is a decreasing function of α according to Eq. (6.15), it is the case that

$$\alpha_{i^b,j^b} < \alpha_{i,\psi(i)}.$$

(C2): As $U_{P_{j,i}}$ is an increasing function of α, it holds that

$$\alpha_{i^b,j^b} > \alpha_{\psi(j),j}.$$

It is clear that (C1) contradicts (C2), and therefore PT_{i^b} and ST_{j^b} are not matched.

C.2 Proof of Lemma 2

The outage probability at l*th* receiver due to the non-colluding eavesdroppers

$$\begin{aligned} P_{o,i} &= \mathbb{P}(\gamma_E \geq \rho_i | \rho_i) \\ &= \int_0^\infty \mathbb{P}\left[\max_{l\in\phi_e} P_p \left|\left(\mathbf{h}_l^{(PE)}\right)^\dagger \mathbf{u}_j'\right|^2 \geq \right. \\ &\quad \left. (\sigma^2 + P_s \left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger \mathbf{v}_j'\right|)\rho_i\right] f_{|E|}(l)dl \\ &= \int_0^\infty \left[\exp(-\frac{N\rho_i\sigma^2\,|l|^\beta}{P_p}) \right. \\ &\quad \mathbb{E}\left(\exp(-N\frac{\rho_i P_s \left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger \mathbf{v}_j'\right|^2}{\overline{P_p\,|l|^{-\beta}}})\right) \left. f_{|E|}(l)dl\right]. \end{aligned} \tag{C.3}$$

According to [97], Eq. (C.3) consists of two terms. The first term, $\exp(-\frac{\rho_i\sigma^2|l|^\beta}{P_p})$, depends only on the noise, whilst the second term, $\mathbb{E}\left(\exp(-\frac{\rho_i|l|^\beta P_s\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger \mathbf{V}_j'\mathbf{h}_l^{(SE)}\right|}{P_p})\right)$, depends on the interference caused by the ST jammer. The second term, denoted by the subscript I, can be solved by a Laplace transform when $s = \frac{P_s N\rho_i|l|^\beta}{P_p}$:

$$\begin{aligned} \mathcal{L}_I &= \exp\left(-2\pi\lambda_e \int_0^\infty \mathbb{E}_h^{SE} \right. \\ &\quad \left. (1-\exp(-s\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger \mathbf{v}_j'\right|^2 |y|^{-\beta}))dy\right) \\ &= \exp\left(-\pi\lambda_e s^{2/\beta}\mathbb{E}[\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger \mathbf{v}_j'\right|^{\frac{2}{\beta}}]\Gamma(1-2/\beta)\right). \end{aligned}$$

(C.4)

Eq. (C.4) follows from the assumption that fading is independent from the PPP, and it is assumed that $\mathbf{h}_l^{(SE)}$ is independent from $\mathbf{v}'_j$. Moreover, it is assumed that $\mathbb{E}[\mathbf{v}'_j] = \exp(1/\sqrt{N})$, and $\mathbb{E}[\left|\mathbf{h}_l^{(SE)}\right|] = 1$ [31]. Consequently, it is possible to substitute $s = \frac{P_s N \rho_i |l|^\beta}{P_p}$ and $\mathbb{E}[\left|\left(\mathbf{h}_l^{(SE)}\right)^\dagger \mathbf{v}'_j\right|^2] = \exp(1/N^{(\frac{1}{\beta})})$ into Eq. (C.4) to obtain the closed-form expression for the interference distribution:

$$\mathbb{E}(I) = \exp\left(-\pi^2 \lambda_e |l|^2 (\frac{P_s N \rho_i}{P_p})^{2/\beta} exp(1/N^{(\frac{1}{\beta})}) \Gamma(1-2/\beta)\right). \tag{C.5}$$

Hence, Eq. (C.5) can be substituted into Eq. (C.3) to obtain the outage probability:

$$\begin{aligned}
P_{o,i} &= \int_0^\infty \Bigg[\exp(-\frac{N\rho_i\sigma^2 |l|^\beta}{P_p}) \\
&\quad \exp\left(-\pi^2 \lambda_e |l|^2 (\frac{P_s N \rho_i}{P_p})^{2/\beta} exp(1/N^{(\frac{1}{\beta})}) \Gamma(1-2/\beta)\right) \\
&\quad f_{|E|}(l) dl\Bigg] \\
&= 2\pi\lambda_e \int_0^\infty \Bigg[\exp\Bigg(-\frac{N\rho_i\sigma^2 |l|^\beta}{P_p} \\
&\quad - |l|^2 (-\pi^2 \lambda_e (\frac{P_s N \rho_i}{P_p})^{2/\beta} \exp(1/N^{(\frac{1}{\beta})}) \Gamma(1-2/\beta))\Bigg) \\
&\quad l dl\Bigg] \qquad \text{(C.6)} \\
&= 2\pi\lambda_e \int_0^\infty \Bigg[\exp\Bigg(-\frac{N\rho_i\sigma^2 u^4}{P_p} \\
&\quad -u^2(\pi^{\frac{3}{2}} \lambda_e \sqrt{\frac{P_s N \rho_i}{P_p}} \\
&\quad \exp(1/N^{-4}))\Bigg) u du\Bigg] \qquad \text{(C.7)} \\
&= \pi\lambda_e \int_0^\infty \Bigg[\exp\Bigg(-\frac{N\rho_i\sigma^2 y^2}{P_p} \\
&\quad -y(\pi^{\frac{3}{2}} \lambda_e \sqrt{\frac{P_s N \rho_i}{P_p}} \\
&\quad \exp(1/N^{-4}))\Bigg) dy\Bigg] \qquad \text{(C.8)} \\
&= \frac{\pi^{\frac{3}{2}} \lambda_e}{2} \sqrt{\frac{P_p}{N\rho_i\sigma^2}} \\
&\quad \exp\left(\frac{P_p(\pi^{\frac{3}{2}} \lambda_e \sqrt{\frac{P_s N \rho_i}{P_p}}}{}\right.
\end{aligned}$$

$$\frac{}{exp(1/N^{-4}))^2}4N\rho_i\sigma^2\Bigg)$$
$$\text{erfc}\left[\frac{(\pi^{\frac{3}{2}}\lambda_e\sqrt{\frac{P_sN\rho_i}{P_p}}}{\frac{\exp(1/N^{-4}))}{2\sqrt{N\rho_i\sigma^2}}}\right]. \tag{C.9}$$

According to [97], Eq. (C.6) holds when the distance between the ith PT and the nearest eavesdropper follows

$$f_E(x) = 2\lambda_e\pi x\exp(-\lambda_e\pi x^2).$$

From Eq. (C.7), Eq. (C.8) can be obtained by letting $u = |l|$, $\beta = 4$ [31], and $y = |x|^2$. Subsequently, Eq. (C.9) can be obtained by the following formula:

$$\int_0^\infty \exp(-bx^2 - cx)dx = \frac{1}{2}\sqrt{\frac{\pi}{b}}\exp\frac{c^2}{4b}\text{erfc}\left(\frac{c}{2\sqrt{b}}\right).$$

C.3 Proof of Lemma 3

The outage probability at the jth SR can be written as:

$$\begin{aligned}
P_{o_E,k} &= \int_0^\infty \Bigg[\mathbb{P}\left(\max_{x\in\phi_e}\frac{P_s\left|\mathbf{h}_x^{(SE)^\dagger}\mathbf{u}_j'\right|^2}{\sigma^2+}\right. \\
&\quad \left.\frac{}{P_s\left|\mathbf{h}_x^{(SE)^\dagger}\mathbf{v}_j'\right|^2}\right) \geq \rho_j|\rho_j\Bigg] f_E(x)dx \\
&= \int_0^\infty \exp(\frac{-N\rho_j\sigma^2x^\beta}{P_s(1-\rho_j)}) \\
&\quad f_E(x)dx \qquad (C.10) \\
&= 2\pi\lambda_e\int_0^\infty\Big[\exp(\frac{-N\rho_j\sigma^2x^\beta}{P_s(1-\rho_j)} \\
&\quad -\lambda_e\pi x^2)xdx\Big] \qquad (C.11) \\
&= 2\pi\lambda_e\int_0^\infty\Bigg[x\exp(\frac{-N\rho_j\sigma^2|x|^4}{P_s(1-\rho_j)}
\end{aligned}$$

$$
\begin{aligned}
& -\lambda_e \pi x^2) dx \Big] && \text{(C.12)} \\
= \; & \pi \lambda_e \int_0^{\infty} \left[\exp(\frac{-N\rho_j \sigma^2 u^2}{P_s(1-\rho_j)} - \lambda_e \pi u) du \right] && \text{(C.13)} \\
= \; & \frac{\pi^{3/2} \lambda_e \sqrt{P_s(1-\rho_j)}}{2\sqrt{N\sigma^2 \rho_j}} \\
& \exp\left[\frac{\pi {\lambda_e}^2 P_s(1-\rho_j)}{4N\sigma^2 \rho_j} \right] \\
& \operatorname{erfc}\left(\frac{\pi \lambda_e \sqrt{P_s(1-\rho_j)}}{2\sqrt{N\sigma^2 \rho_j}} \right), && \text{(C.14)}
\end{aligned}
$$

where Eq. (C.10) follows from the PPP distribution of the eavesdroppers. According to [97], Eq. (C.11) holds when the distance between the kth ST and the nearest eavesdropper follows

$$f_E(x) = 2\lambda_e \pi x \exp(-\lambda_e \pi x^2).$$

In Eq. (C.12), letting $\alpha = 4$ and $u = x^2$ yields Eq. (C.13). Subsequently, Eq. (C.14) can be obtained by the following formula:

$$\int_0^{\infty} \exp(-bx^2 - cx) dx = \frac{1}{2}\sqrt{\frac{\pi}{b}} \exp \frac{c^2}{4b} \operatorname{erfc}\left(\frac{c}{2\sqrt{b}} \right).$$

C.4 Proof of Lemma 4

The mean secrecy rate when $\rho_k > \gamma_{e,k}$ can be written as follows:

$$
\begin{aligned}
\mathbb{E}_{\phi_e}[R_k | \rho_k > \gamma_{e,k}] \; = \; & \mathbb{E}_{\phi_e}\left[\max[\zeta(\log_2(1+\rho_k) \right. \\
& \left. - \log_2(1+\gamma_{e,k}))] \right] \\
= \; & \mathbb{E}_{\phi_e}\left[\zeta(\log_2(1+\rho_k) \right. \\
& \left. - \log_2(1+\gamma_{e,k}))] \, \mathbb{1}_{(\gamma_{e,k} < \rho_k)} \right. \\
= \; & \zeta(\mathbb{E}_{\phi_e}(\log_2(1+\rho_k) \mathbb{1}_{(\gamma_{e,k} < \rho_k)} - \mathbb{E}_{\phi_e} \\
& \log_2(1+\gamma_{e,k}) \mathbb{1}_{(\gamma_{e,k} < \rho_k)}) && \text{(C.15)} \\
= \; & \zeta(\mathbb{P}(\gamma_{e,k} < \rho_k) \log_2(1+\rho_k) \\
& - \mathbb{P}(\gamma_{min} < \gamma_{e,k} < \rho_k) \\
& \log_2(1+\gamma_{e,k})) \\
= \; & \zeta(\log_2(1+\rho_k)^{1-P_{o_{E,k}}}
\end{aligned}
$$

$$-\int_{\gamma_{min}}^{\rho_k} f_{\gamma_e}(x)\log_2(1+x))dx. \tag{C.16}$$

The primary secrecy rate, $f_{\gamma_e}(x)$, can be written as

$$\begin{aligned} f_{\gamma_e}(x) &= \frac{1}{2\sqrt{\pi}g^2x^{5/2}} \\ &\left[\exp\left(-\frac{b^2(-p)+\frac{2c\left(d\sqrt{p}-bp\right)}{\sqrt{x}}+d^2}{g^2}\right)\right. \\ &\left(2acg\sqrt{p}\sqrt{x}-\sqrt{\pi}a\left(2bcp\sqrt{x}+2c^2p+g^2x\right)\right. \\ &e^{\frac{\left(c\sqrt{p}+d\sqrt{x}\right)^2}{g^2x}} \\ &\left.\left.\operatorname{erfc}\left(\frac{\frac{c\sqrt{p}}{\sqrt{x}}+d}{g}\right)\right)\right]. \end{aligned} \tag{C.17}$$

The secondary secrecy rate, $f_{\gamma_e}(x)$, can be written as

$$\begin{aligned} f_{\gamma_e}(x) &= \frac{ae^{-\frac{(x-1)\left(b-c^2\right)}{x}}}{2\sqrt{\pi}\sqrt{\frac{1}{x}-1}x^3} \\ &\left(\sqrt{\pi}(2b(x-1)-x)e^{c^2\left(\frac{1}{x}-1\right)}\operatorname{erfc}\left(c\sqrt{\frac{1}{x}-1}\right)+2cx\sqrt{\frac{1}{x}-1}\right) \end{aligned} \tag{C.18}$$

where $\mathbb{1}_{(.)}$ is an indicator function in Eq. (C.15). Additionally, $\gamma_{e,k}$ is the SINR at the central processing point with respect to the kth user and represents the worst case of eavesdropping. In Eq. (C.16), $P_{o_E,k}$ is given by $\mathbb{P}(\gamma_{E,k} \geq \gamma_k)$.